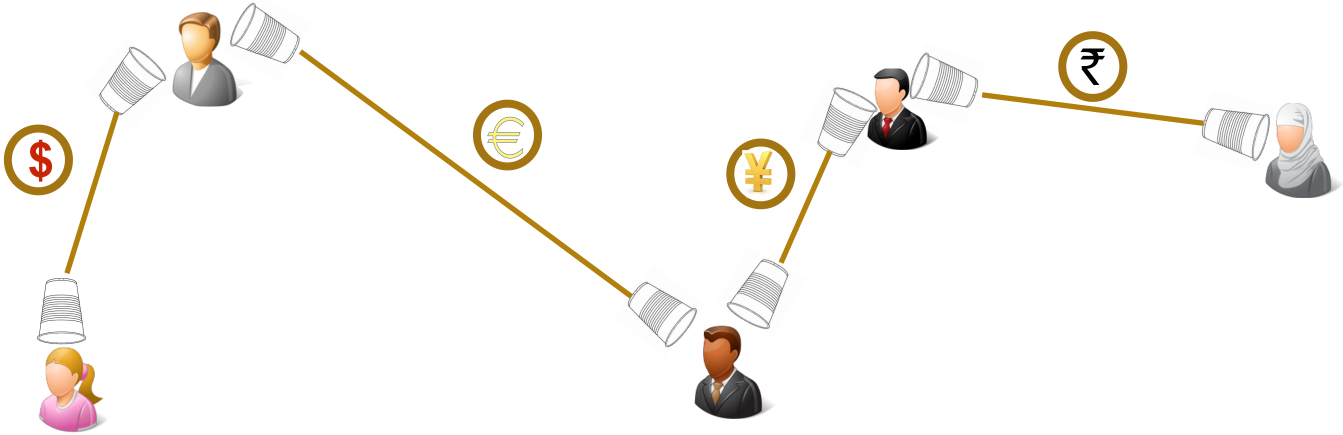
# SilentWhispers: Enforcing Security and Privacy in Decentralized Credit Networks



Giulio Malavolta
Saarland University

**Pedro Moreno-Sanchez**
Purdue University

Aniket Kate
Purdue University

Matteo Maffei
TU Vienna

***NDSS 2017***

# Yet Another Talk about Cryptocurrencies?

- TumbleBit and CoinShuffle++ are excellent ideas to provide privacy in Bitcoin

# Yet Another Talk about Cryptocurrencies?

- TumbleBit and CoinShuffle++ are excellent ideas to provide privacy in Bitcoin

- Bitcoin (as other permissionless cryptocurrencies) relies on a blockchain:
  - High storage requirement (>100 GB)
  - High power consumption for proof-of-work

# Yet Another Talk about Cryptocurrencies?

- TumbleBit and CoinShuffle++ are excellent ideas to provide privacy in Bitcoin

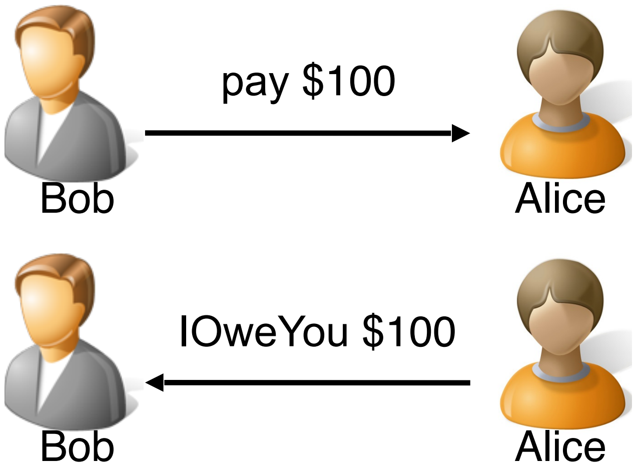
- Bitcoin (as other permissionless cryptocurrencies) relies on a blockchain:
  - High storage requirement (>100 GB)
  - High power consumption for proof-of-work

Is it possible to have a decentralized payment system without a blockchain?

# Credit (or IOU Settlement) Networks: Basics

# Credit (or IOU Settlement) Networks: Basics

## Transactions in the real world



Bob

pay $100

Alice

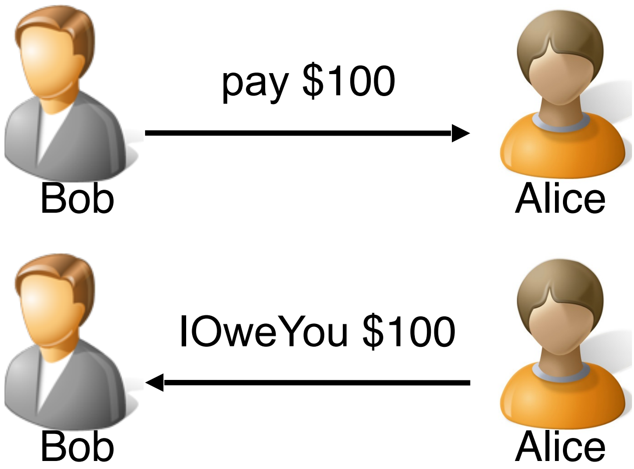
Bob

IOweYou $100

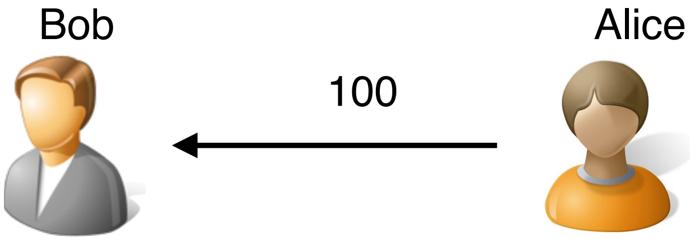
Alice

# Credit (or IOU Settlement) Networks: Basics

## Transactions in the real world

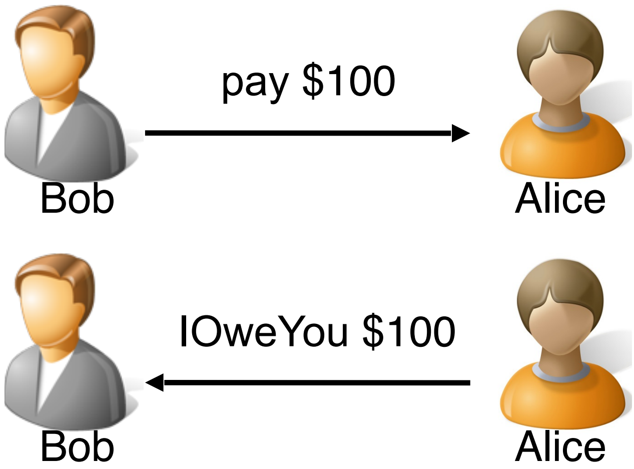


## A credit network representation



# Credit (or IOU Settlement) Networks: Basics

## Transactions in the real world



pay $100

Bob

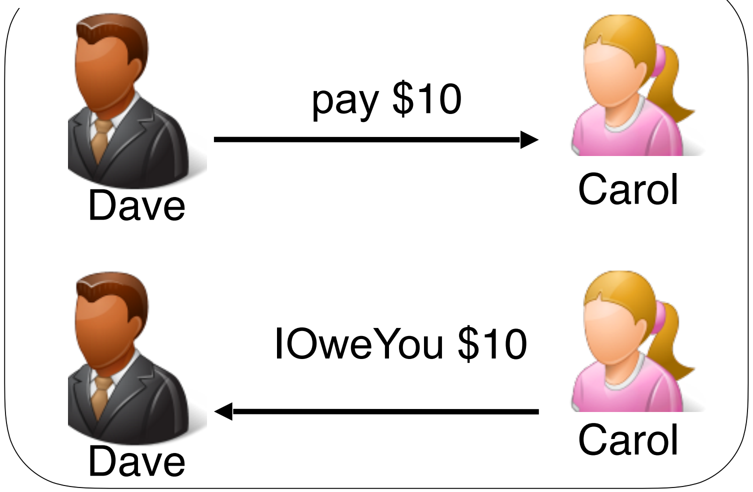
Alice

IOweYou $100

Bob

Alice

During a hike with Alice & Bob



pay $10

Dave

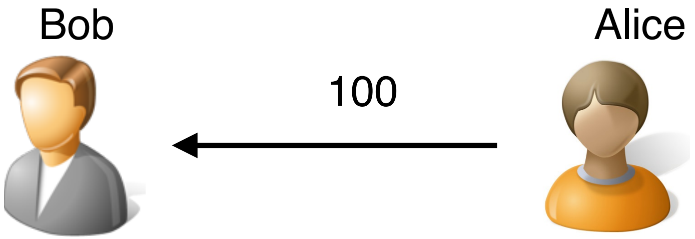
Carol

IOweYou $10

Dave

Carol

## A credit network representation



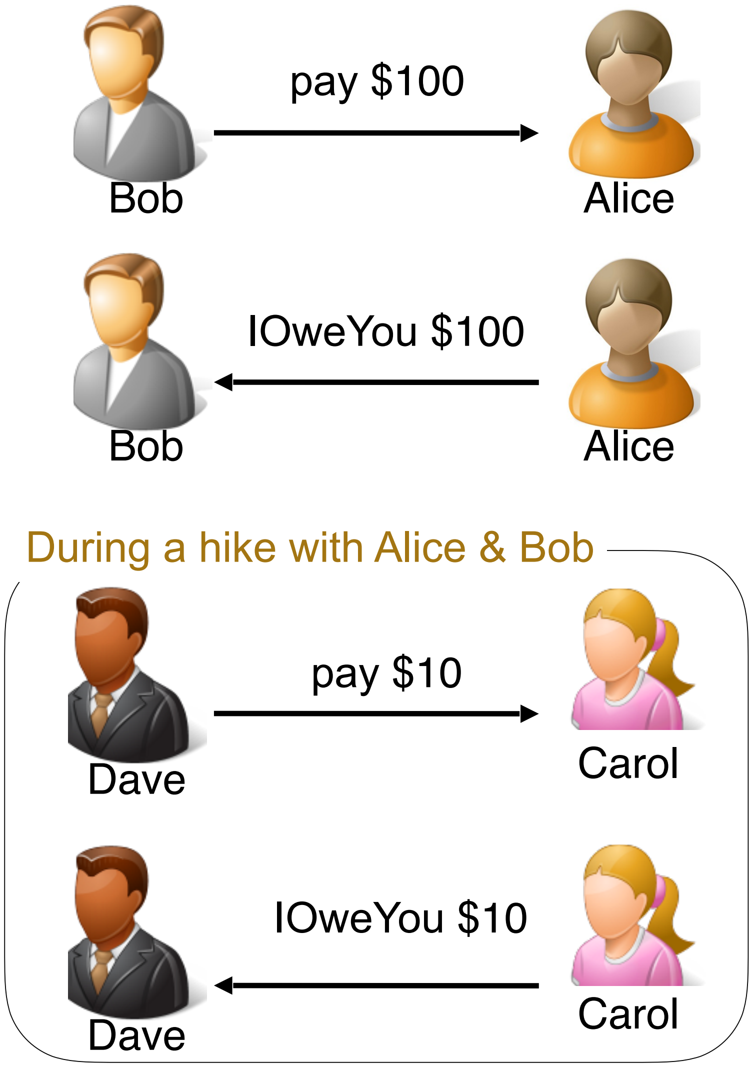
Bob

100

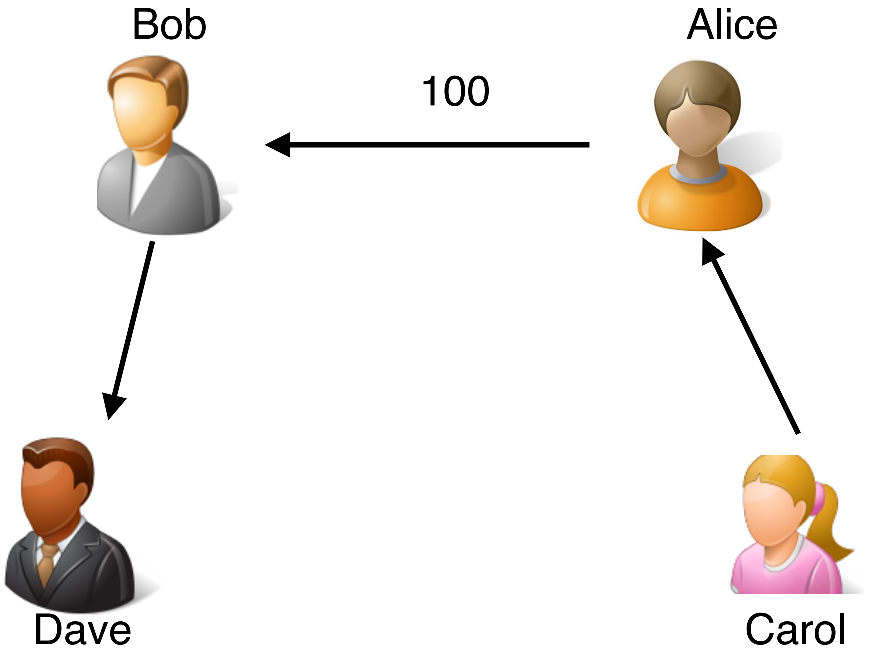
Alice

# Credit (or IOU Settlement) Networks: Basics

## Transactions in the real world

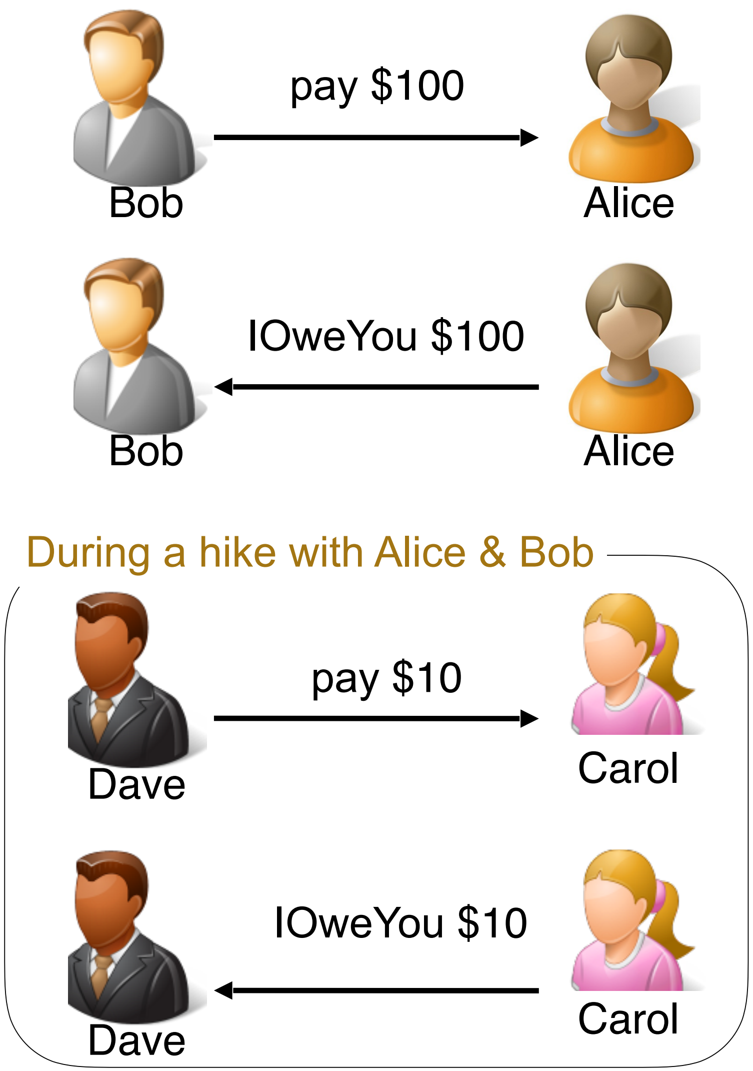


## A credit network representation



# Credit (or IOU Settlement) Networks: Basics

## Transactions in the real world



Bob pay $100 Alice

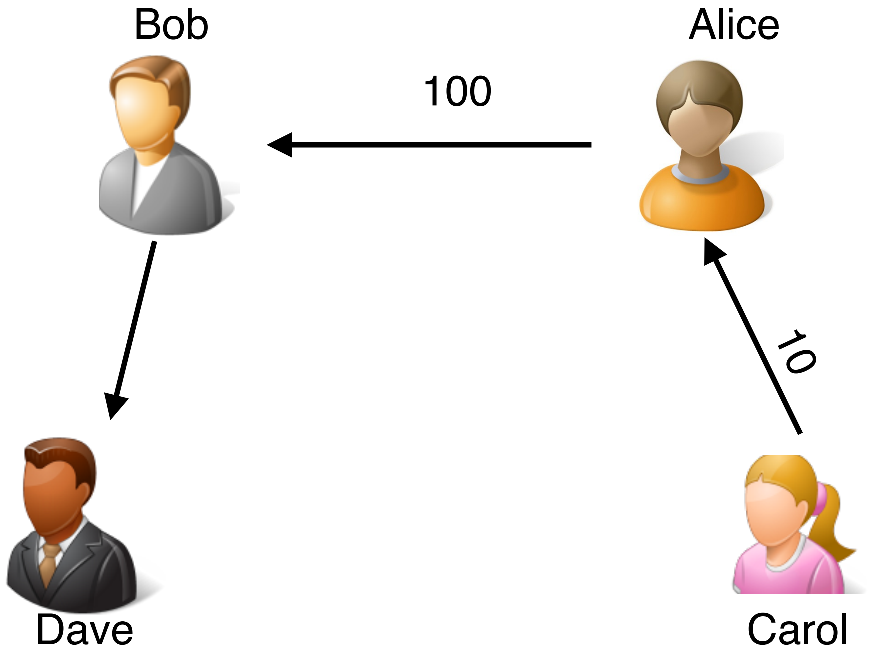
Bob IOweYou $100 Alice

During a hike with Alice & Bob

Dave pay $10 Carol

Dave IOweYou $10 Carol

## A credit network representation



Bob

Alice

100

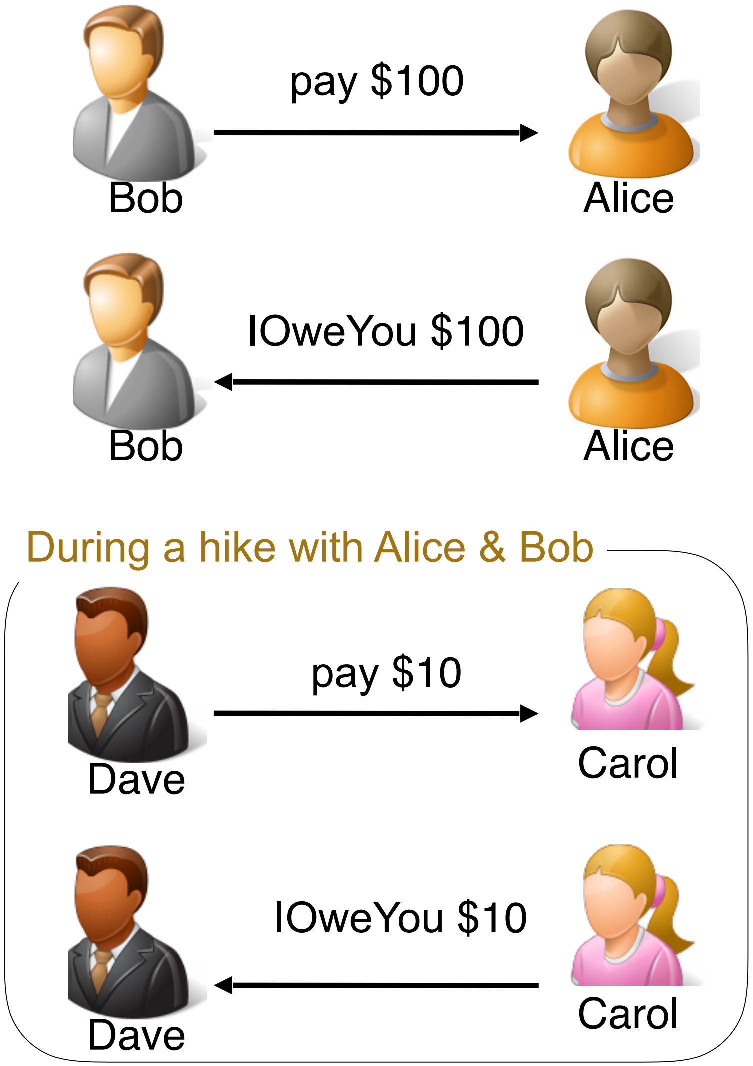
10

Dave

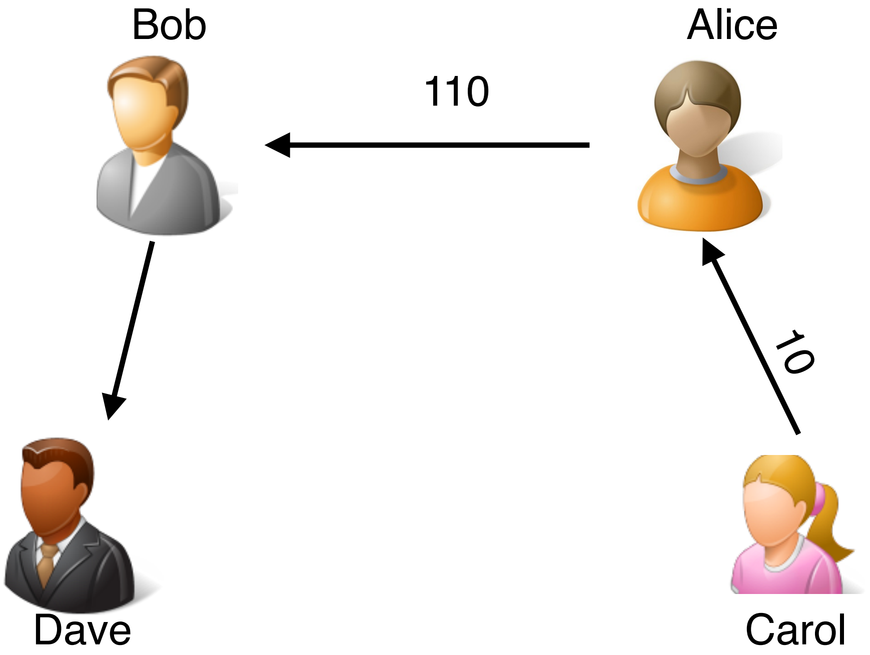
Carol

# Credit (or IOU Settlement) Networks: Basics

## Transactions in the real world

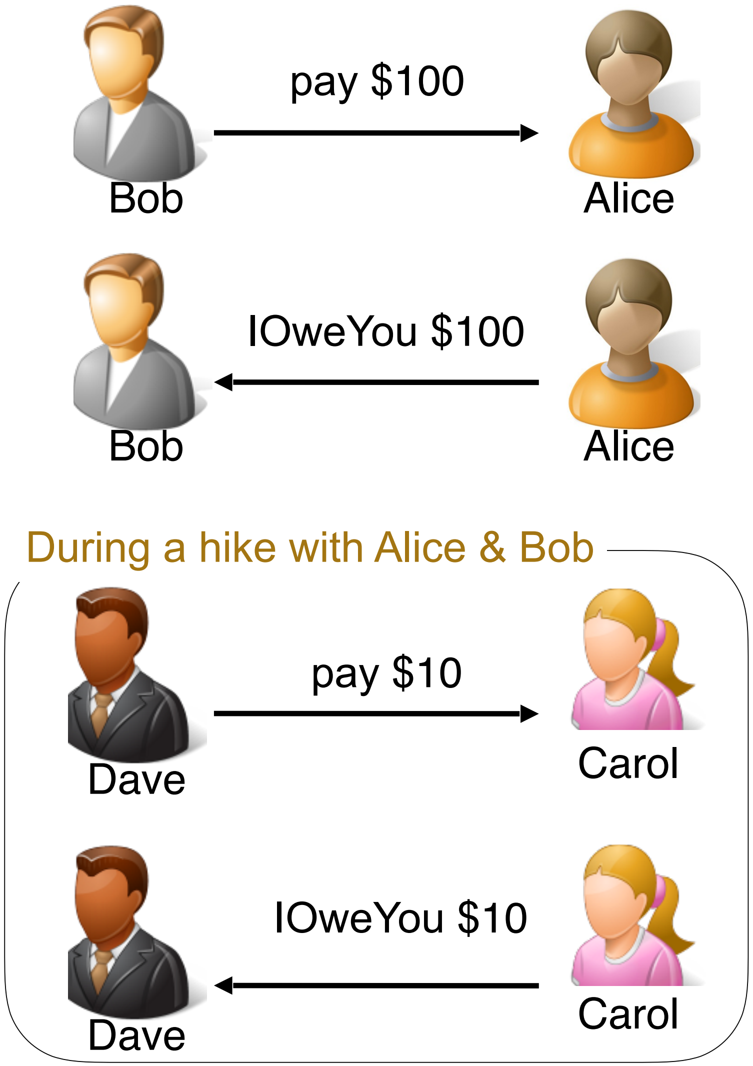


## A credit network representation

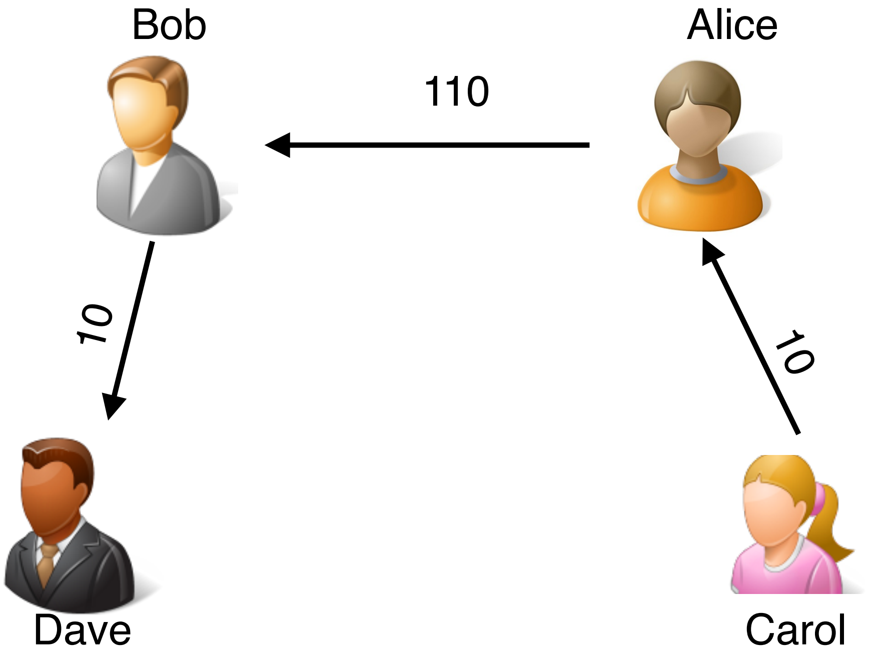


# Credit (or IOU Settlement) Networks: Basics

## Transactions in the real world



## A credit network representation



# Credit Network Examples

- Academic proposals:
  - Ostra: preventing e-mail spam [NSDI'08]

  - Bazaar: strengthening e-commerce [NSDI'11]
  - SumUp: Sybil-resilient content voting [NSDI'09]

- Industry deployments:
  - Ripple: A real-life online payment network
  - Stellar: Another real-life online payment network

# Credit Network Examples

- Academic proposals:
  - Ostra: preventing e-mail spam [NSDI'08]

Sent Mail

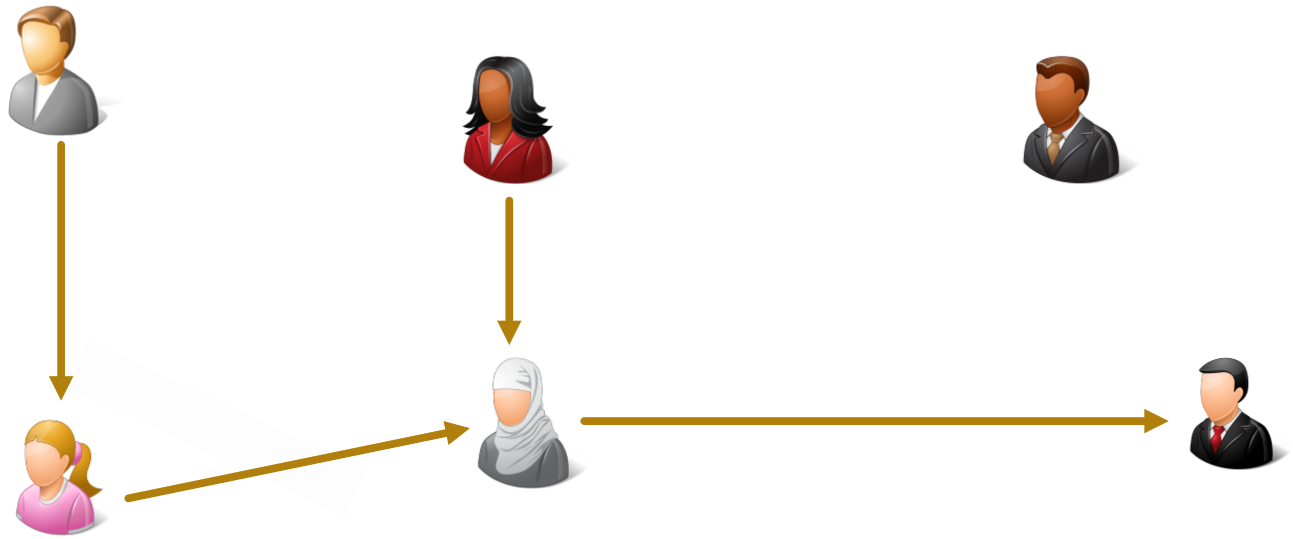
Spam (372)

Trash

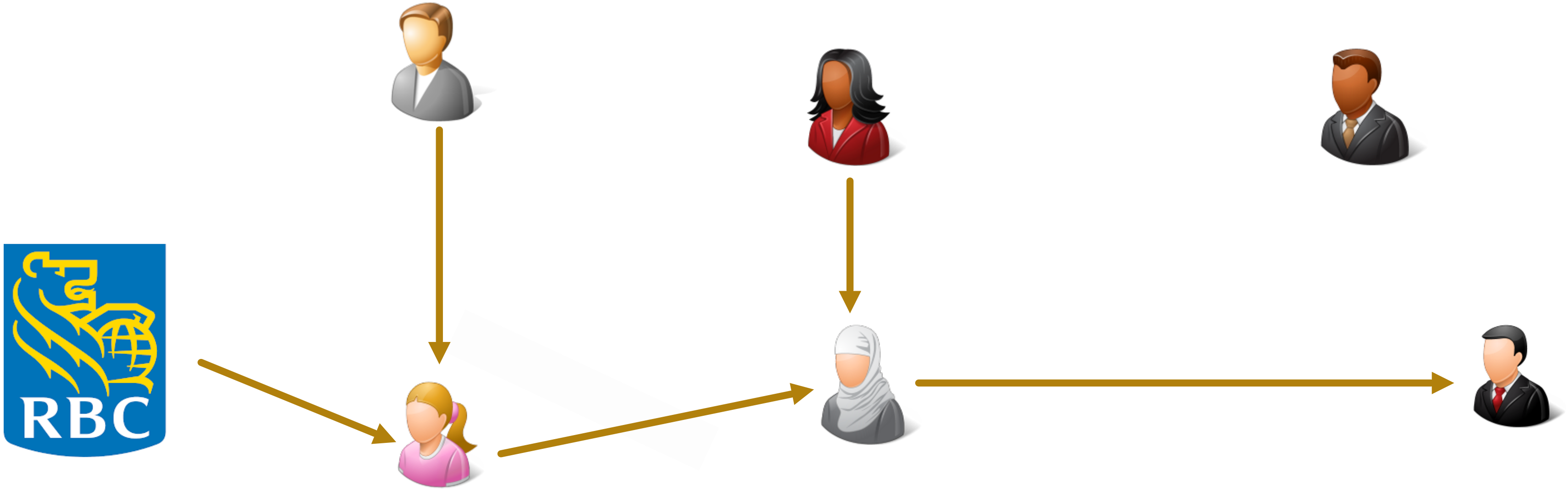
  - Bazaar: strengthening e-commerce [NSDI'11]
  - SumUp: Sybil-resilient content voting [NSDI'09]

- Industry deployments:
  - Ripple: A real-life online payment network
  - Stellar: Another real-life online payment network

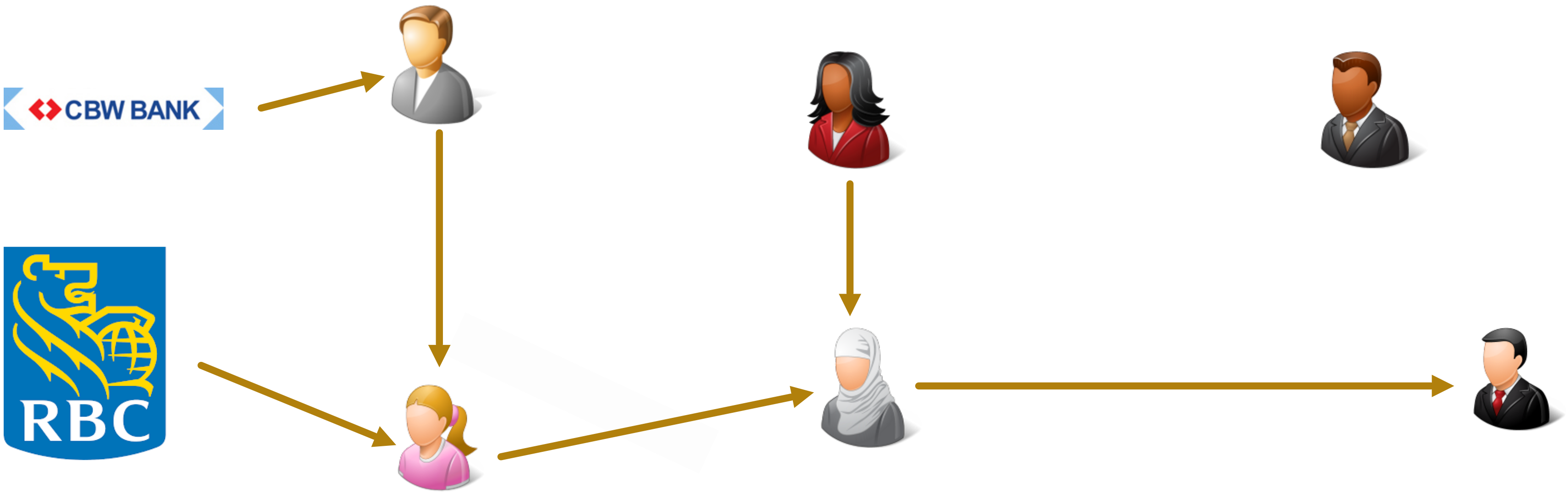
# Ripple Credit Network



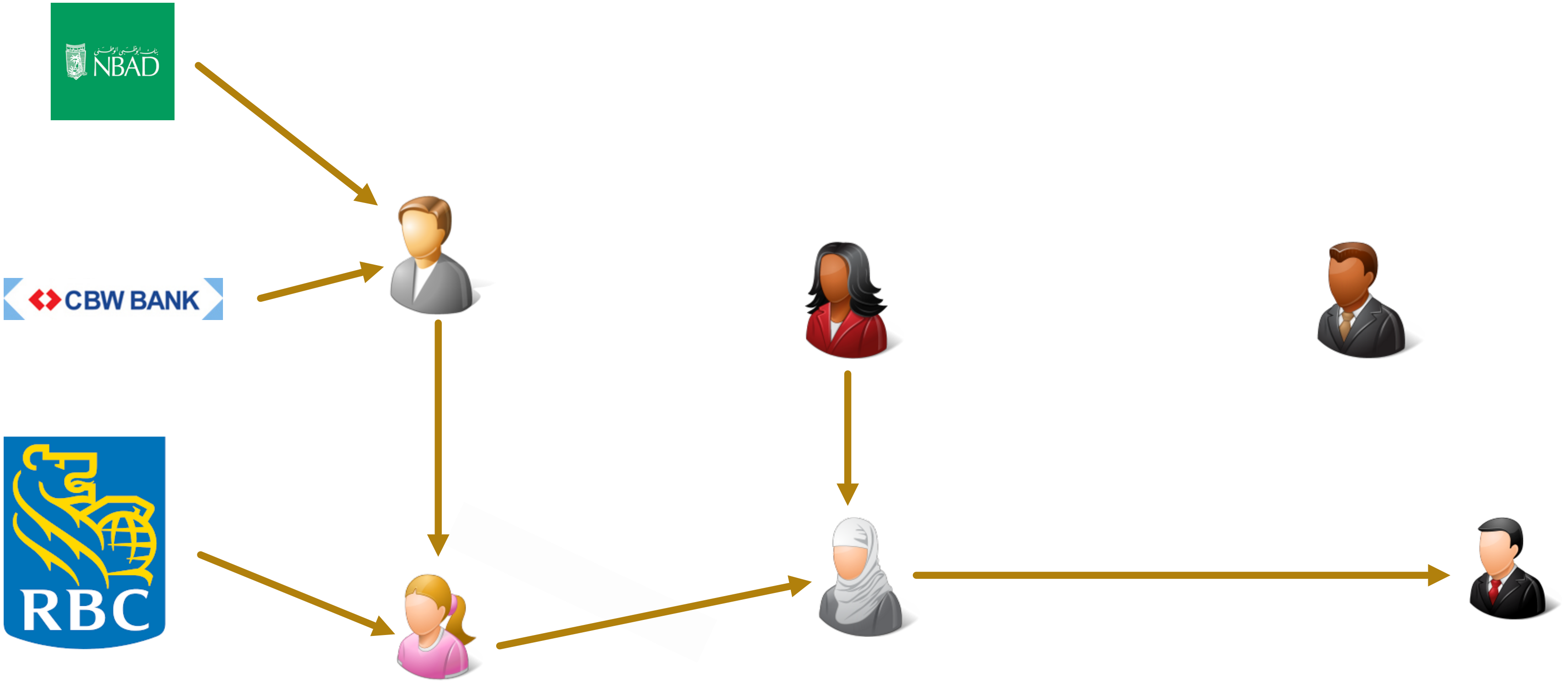
# Ripple Credit Network



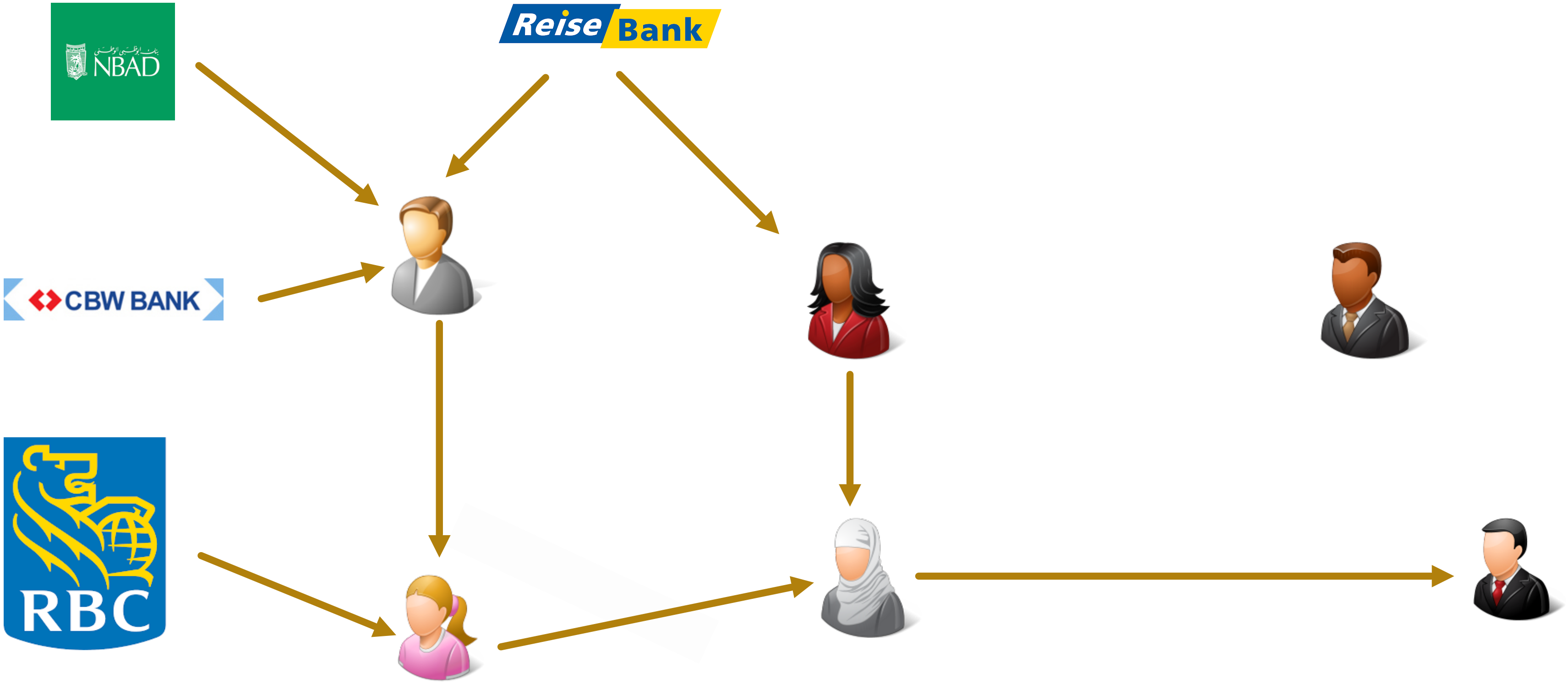
# Ripple Credit Network



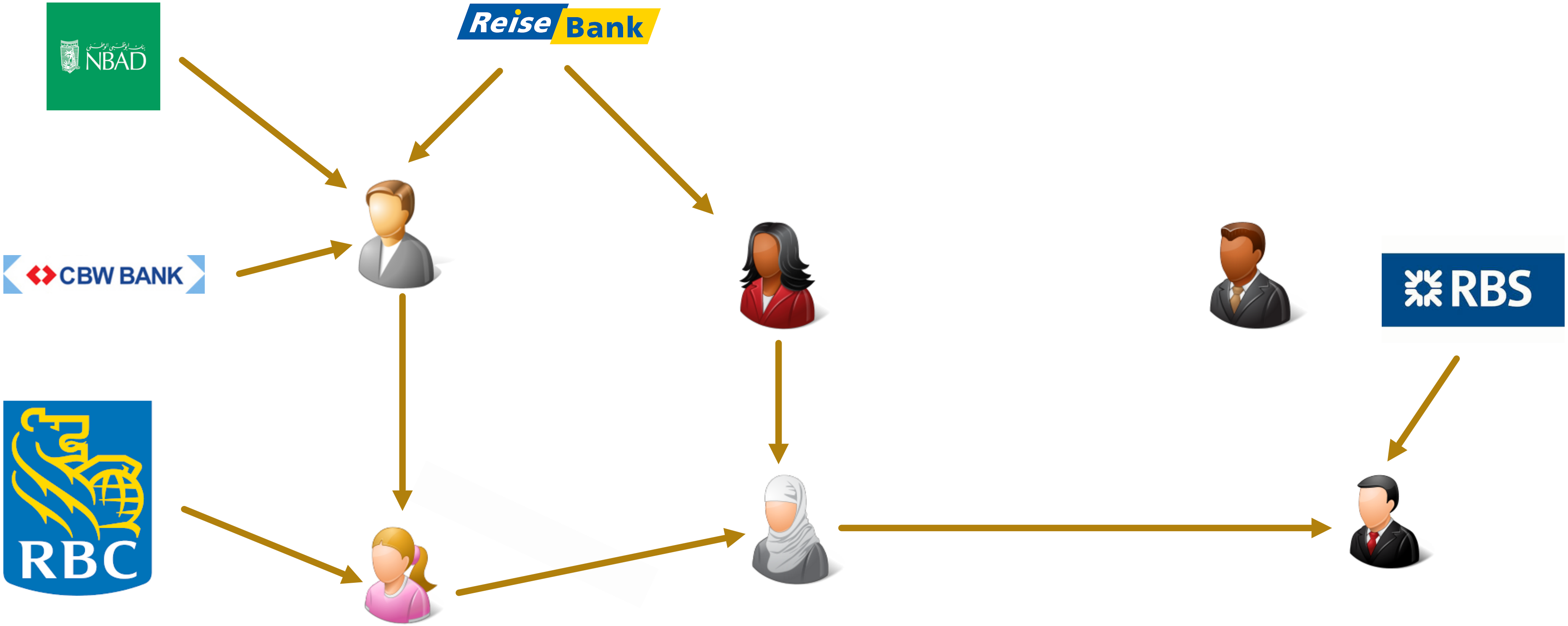
# Ripple Credit Network



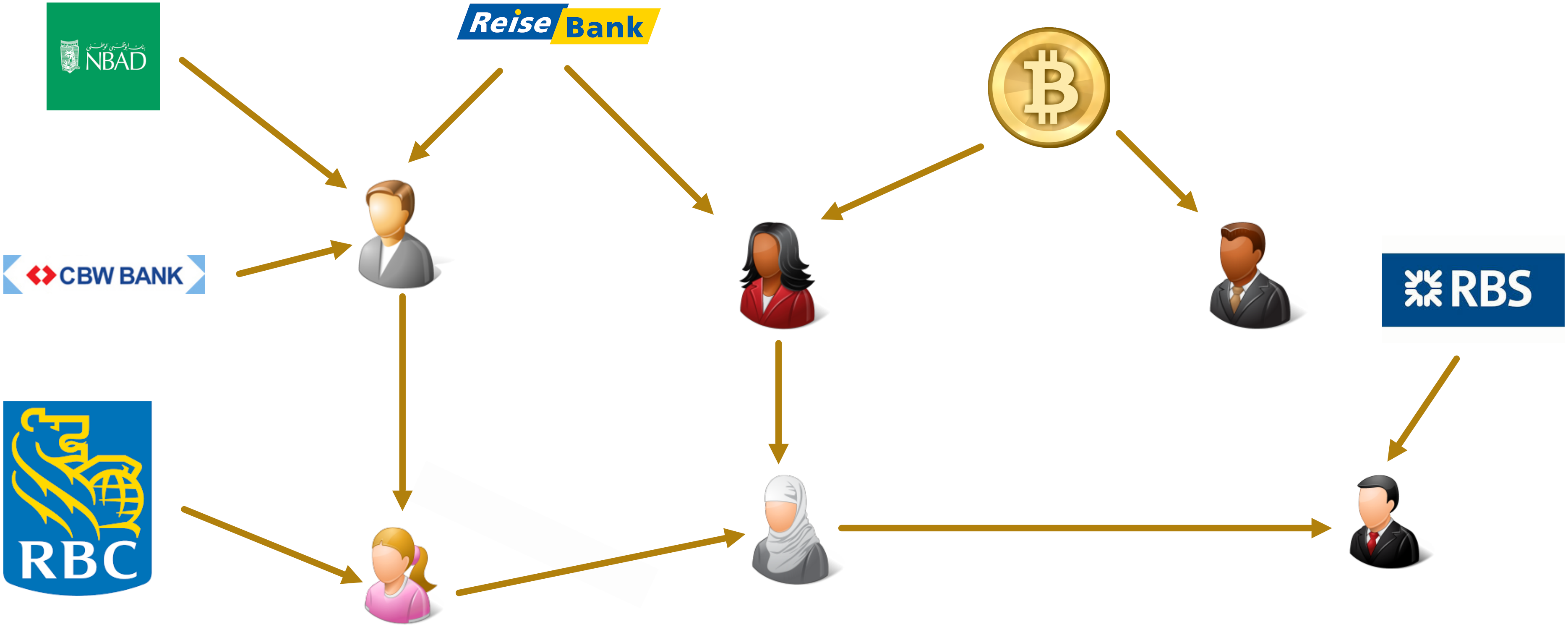
# Ripple Credit Network



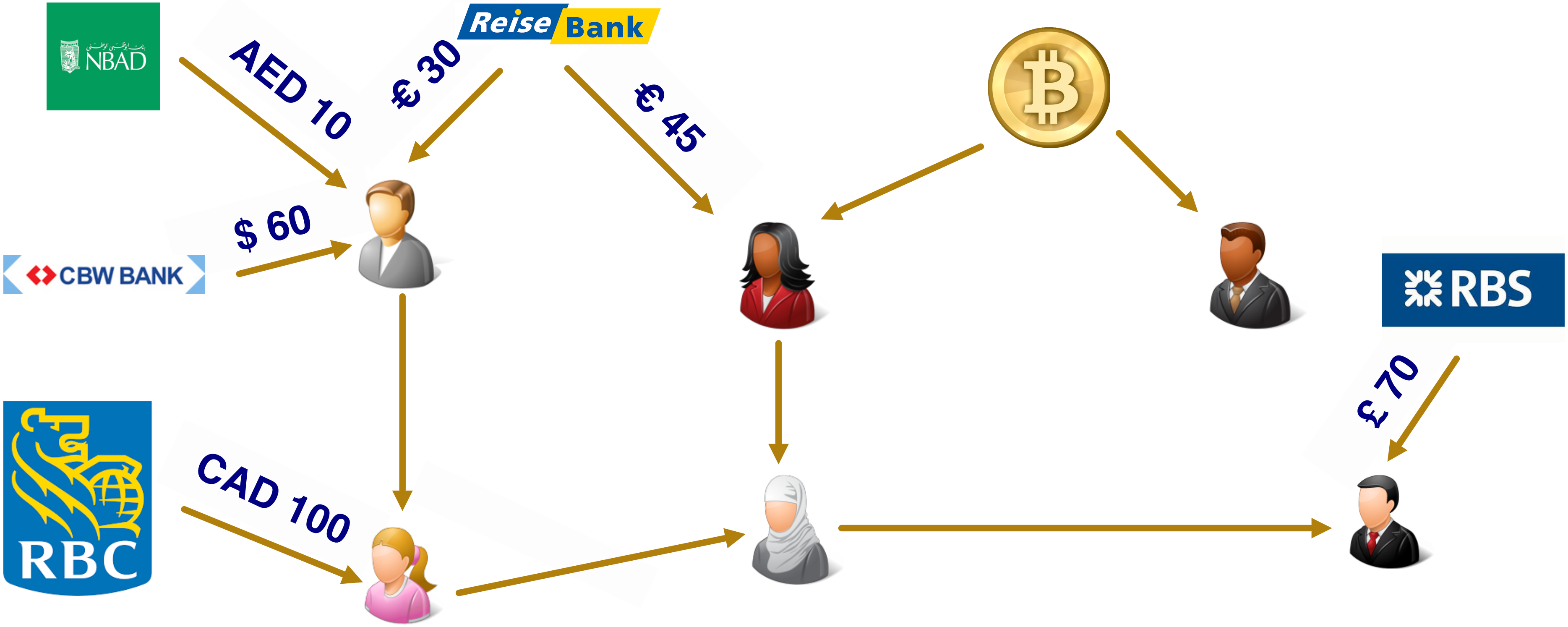
# Ripple Credit Network



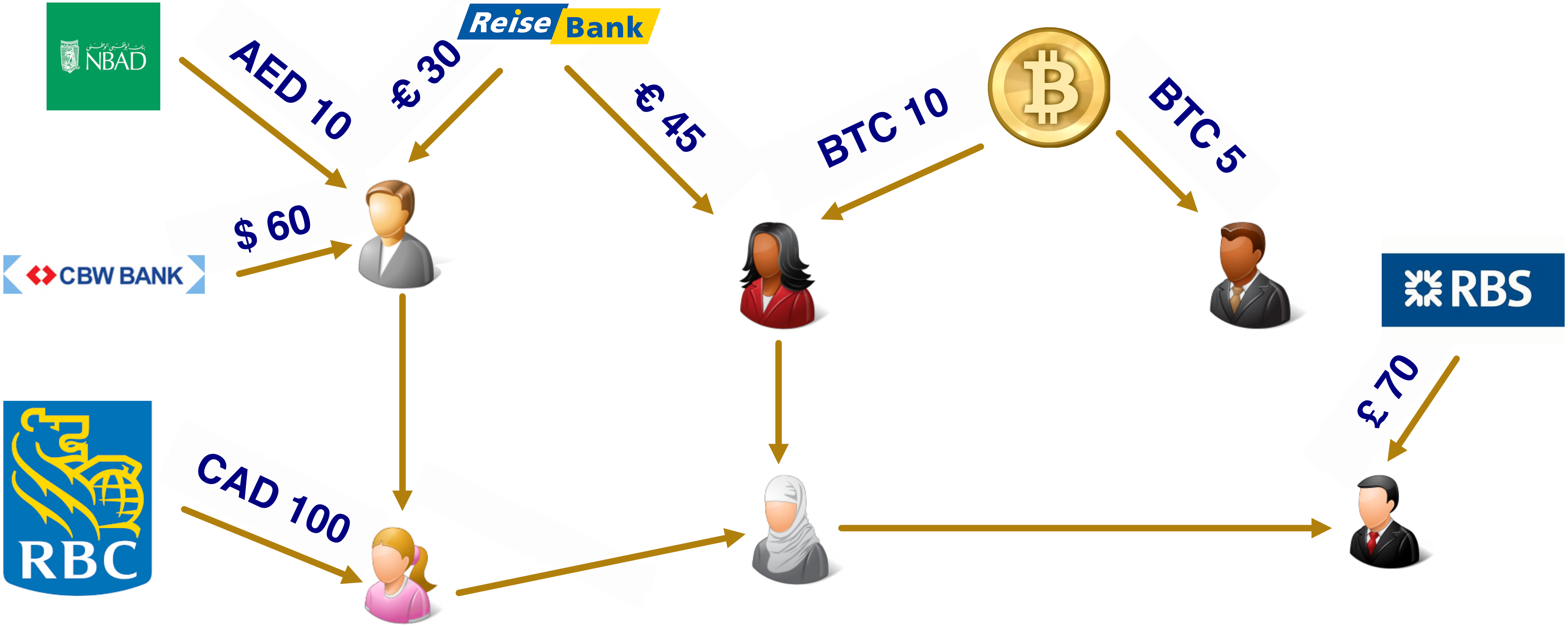
# Ripple Credit Network



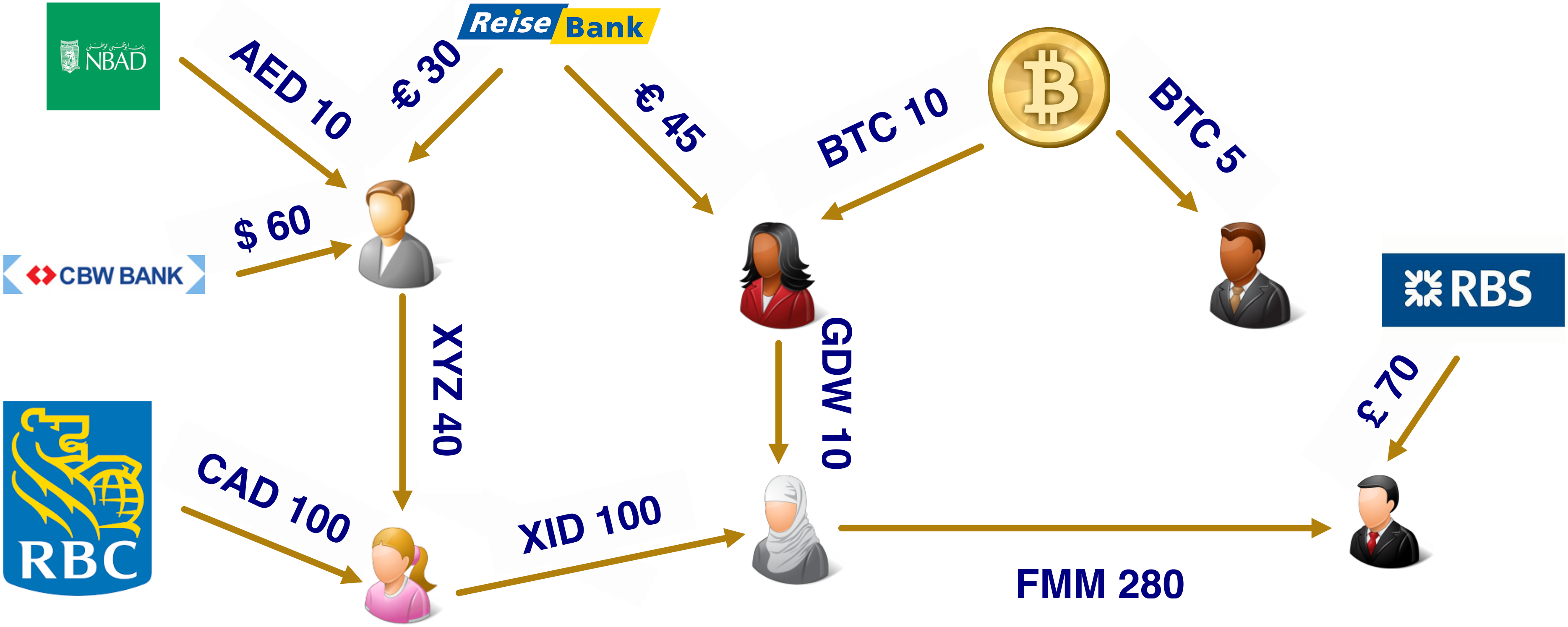
# Ripple Credit Network



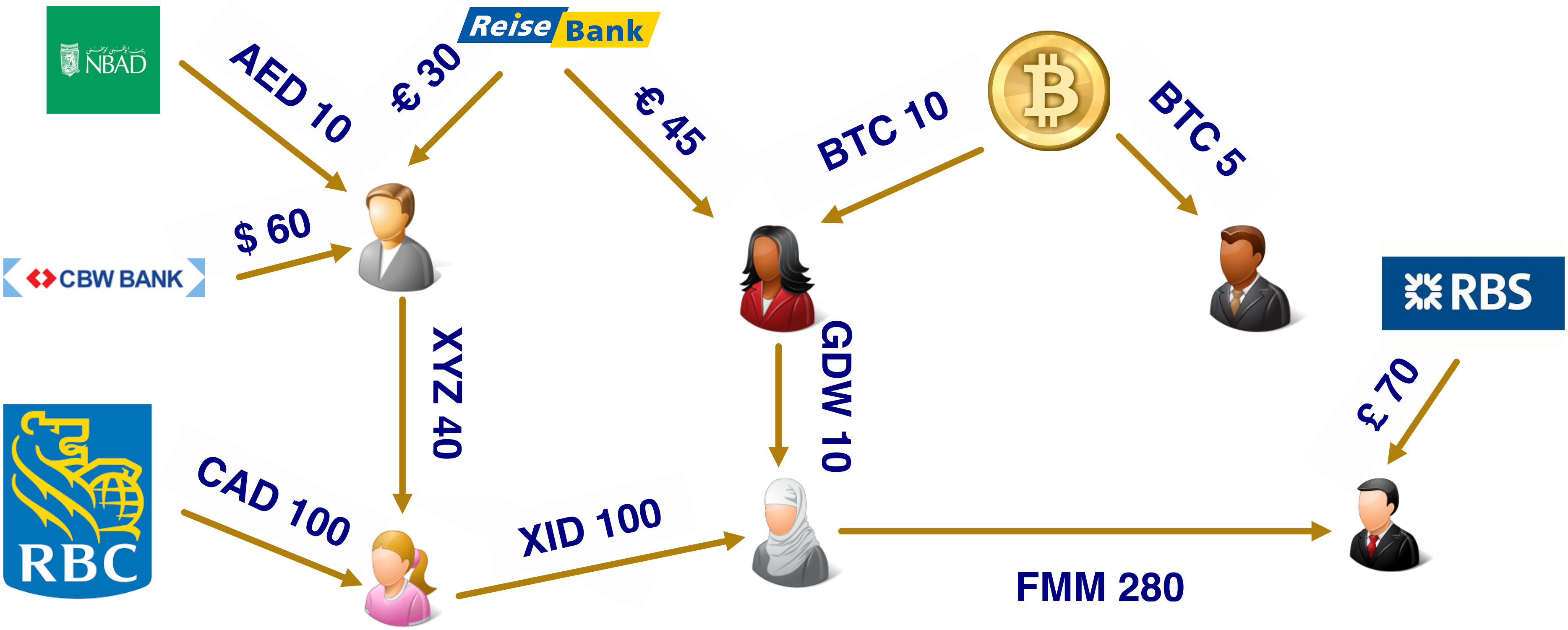
# Ripple Credit Network



# Ripple Credit Network



# Ripple Credit Network

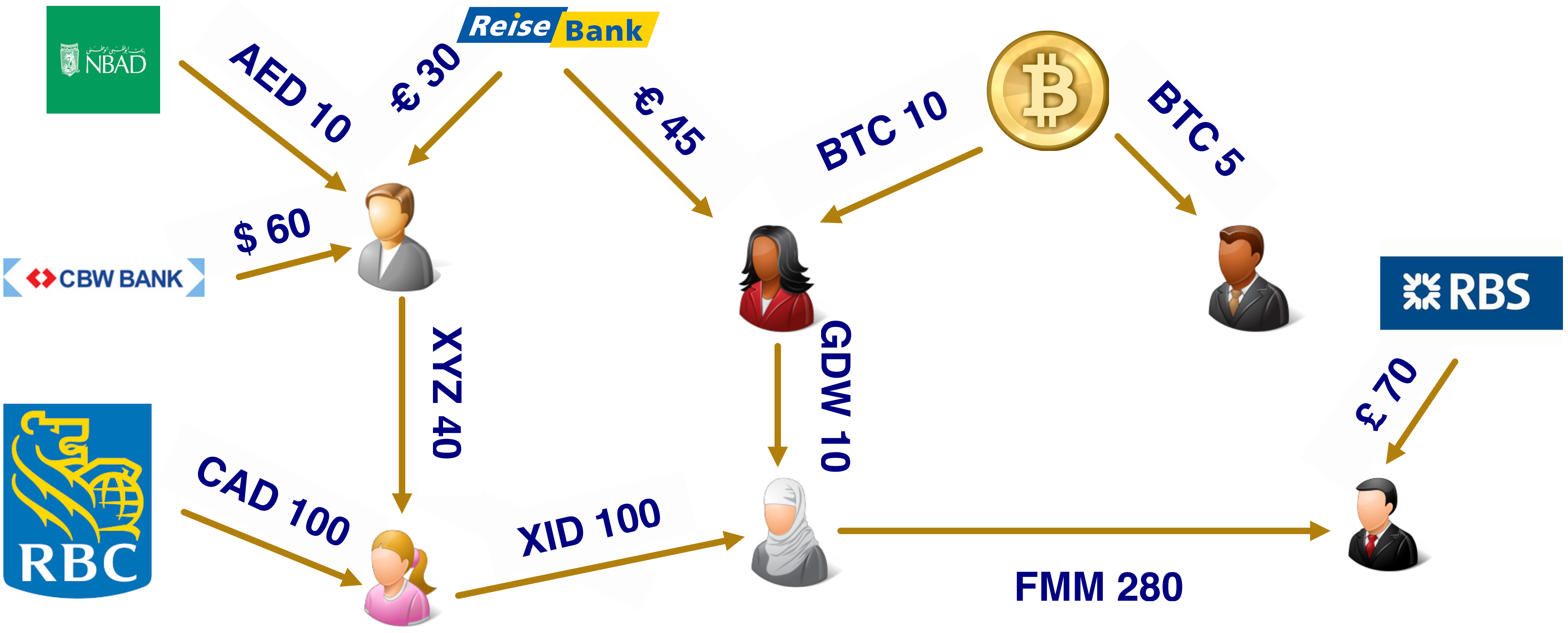


Tx time

Worldwide,
cross-currency tx

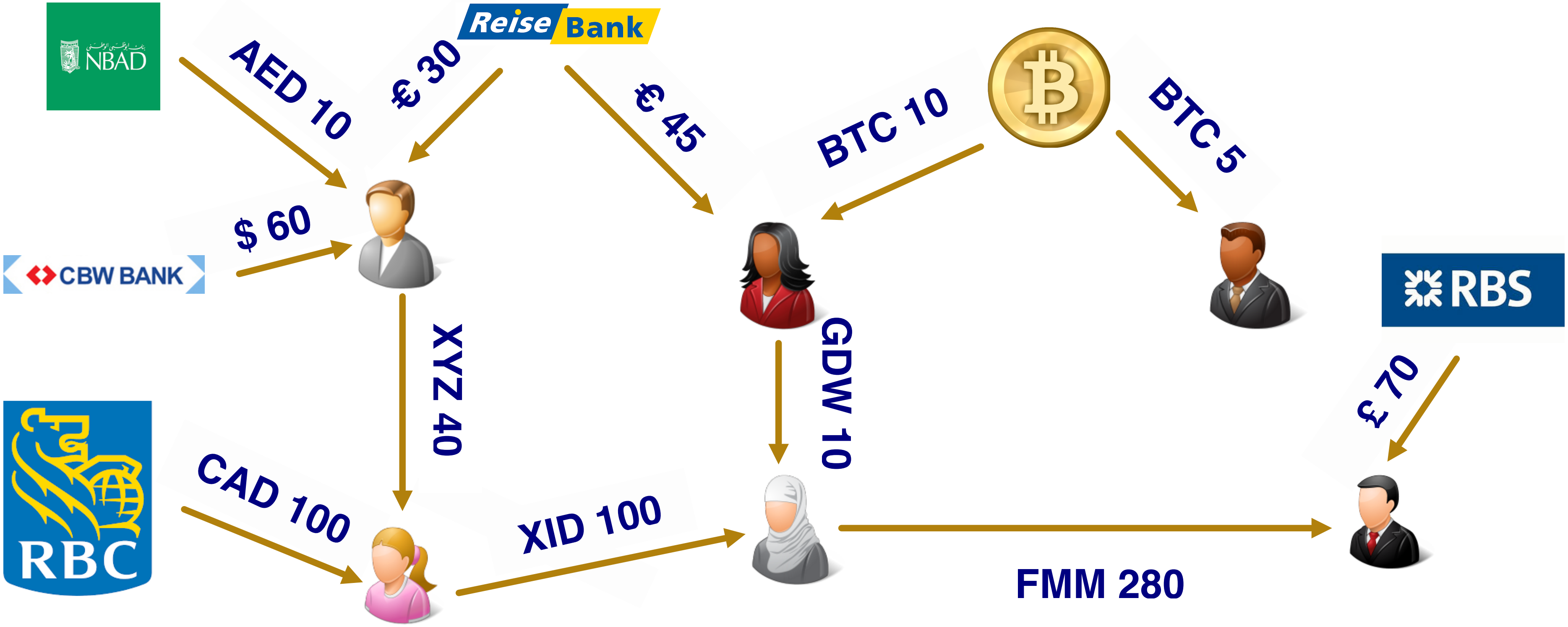
Integrity

# Ripple Credit Network



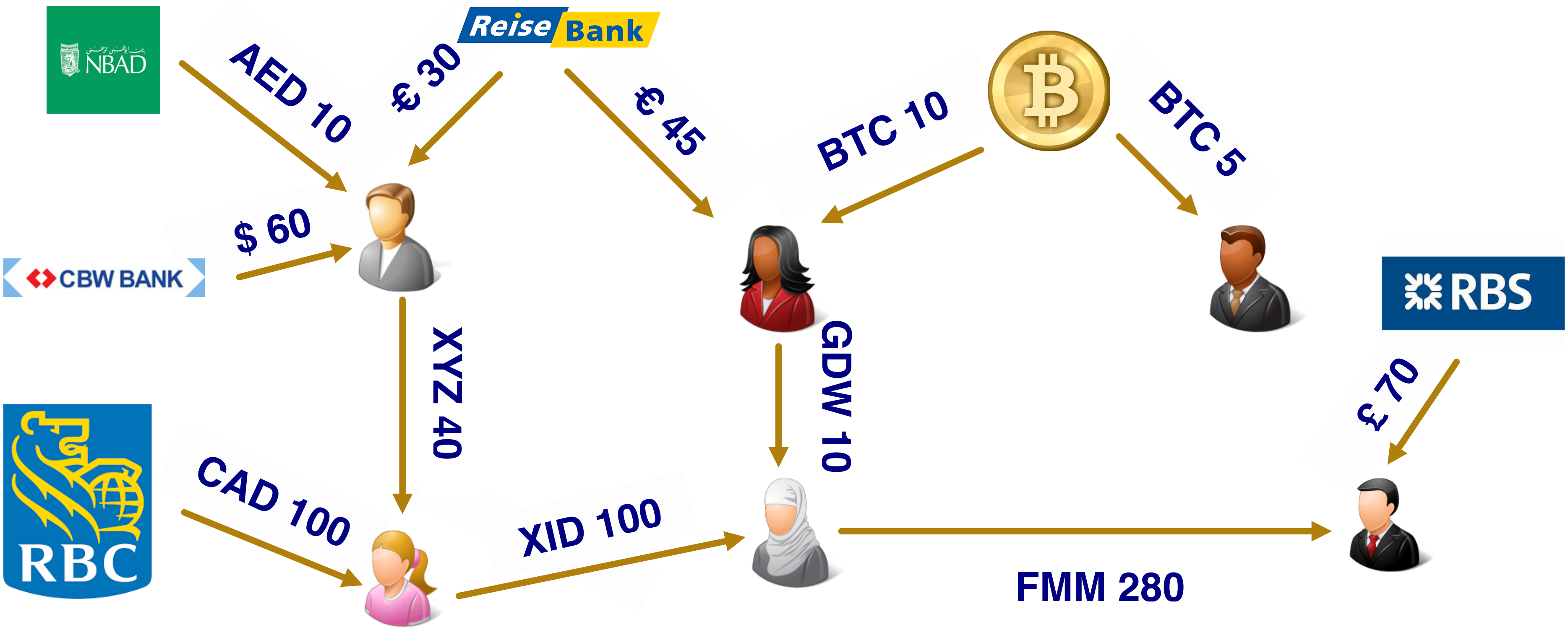
| | Tx time | Worldwide, cross-currency tx | Integrity |
|---|---|---|---|
| BANK | ~ 1 day | | |
| ripple | ~ 5 seconds | | |

# Ripple Credit Network



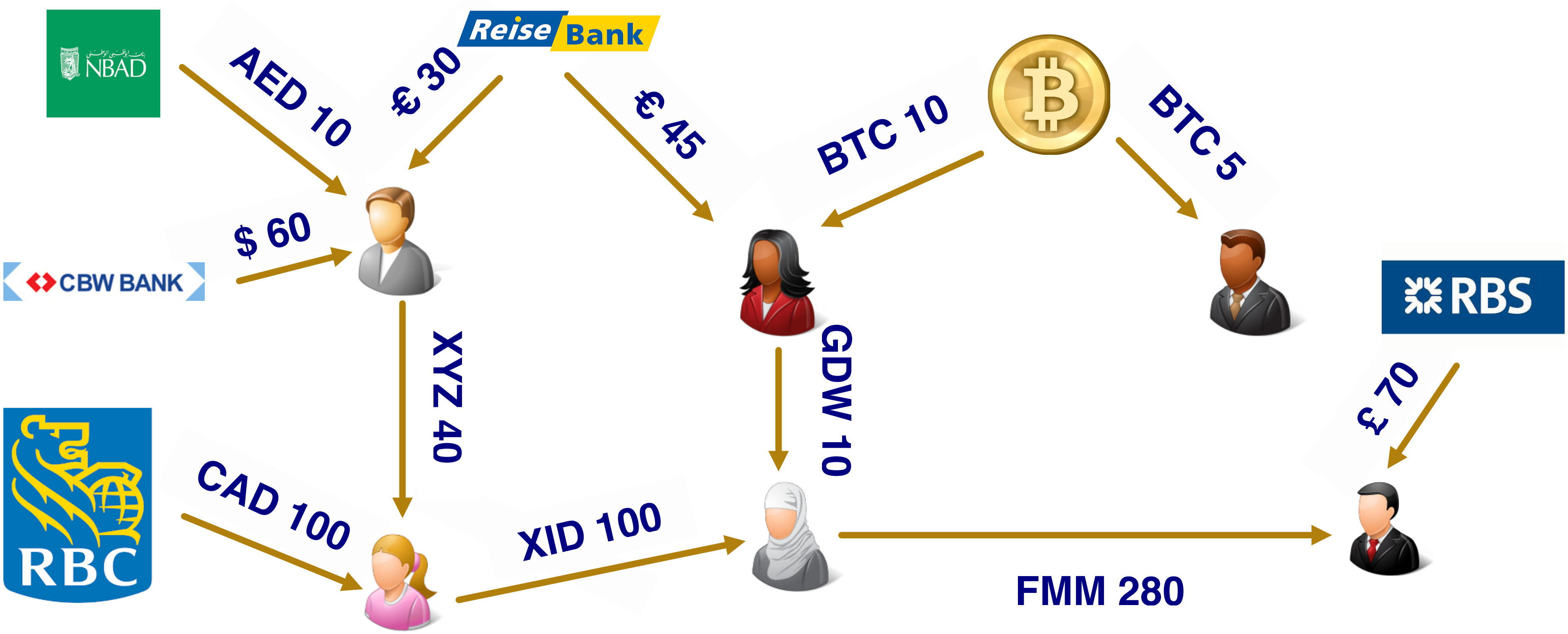
| | Tx time | Worldwide, cross-currency tx | Integrity |
|---|---|---|---|
| BANK | ~ 1 day | High fees | |
| ripple | ~ 5 seconds | Tiny fees | |

# Ripple Credit Network



| | Tx time | Worldwide, cross-currency tx | Integrity |
|---|---|---|---|
| BANK | ~ 1 day | High fees | Bank only |
| ripple | ~ 5 seconds | Tiny fees | Public verifiability |

# Ripple Credit Network



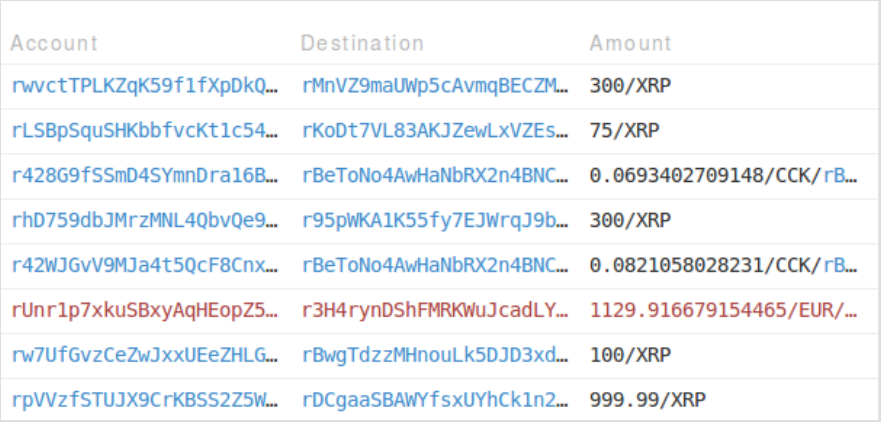
| | Tx time | Worldwide, cross-curr | Integrity |
|---|---|---|---|
| BANK | ~ 1 d | | Bank only |
| ripple | ~ 5 seco | iny fees | Public verifiability |

Ripple can significantly improve cross-currency remittance and settlements

# Public Verifiability & Privacy Problem

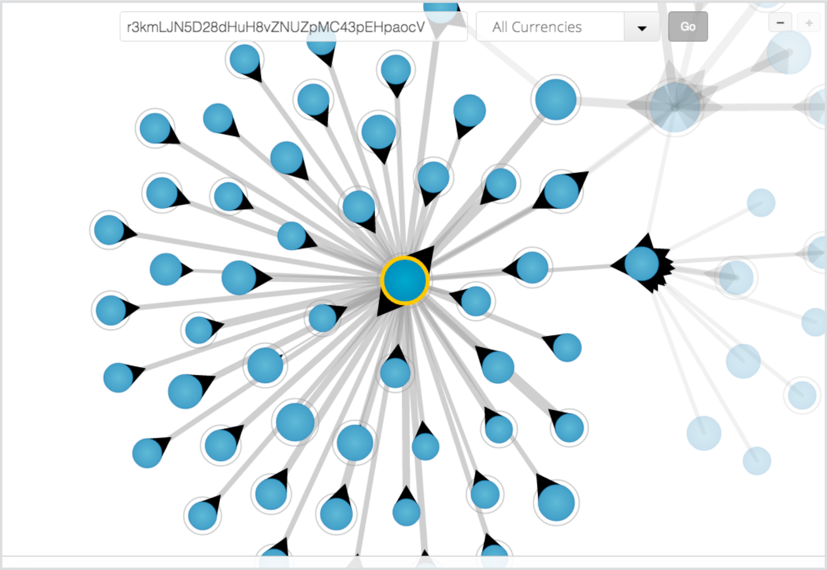
## The Ripple Ledger

### Transaction Details



| Account | Destination | Amount |
|---|---|---|
| rwvctTPLKZqK59f1fXpDkQ… | rMnVZ9maUWp5cAvmqBECZM… | 300/XRP |
| rLSBpSquSHKbbfvcKt1c54… | rKoDt7VL83AKJZewLxVZEs… | 75/XRP |
| r428G9fSSmD4SYmnDra16B… | rBeToNo4AwHaNbRX2n4BNC… | 0.0693402709148/CCK/rB… |
| rhD759dbJMrzMNL4QbvQe9… | r95pWKA1K55fy7EJWrqJ9b… | 300/XRP |
| r42WJGvV9MJa4t5QcF8Cnx… | rBeToNo4AwHaNbRX2n4BNC… | 0.0821058028231/CCK/rB… |
| rUnr1p7xkuSBxyAqHEopZ5… | r3H4rynDShFMRKWuJcadLY… | 1129.916679154465/EUR/… |
| rw7UfGvzCeZwJxxUEeZHLG… | rBwgTdzzMHnouLk5DJD3xd… | 100/XRP |
| rpVVzfSTUJX9CrKBSS2Z5W… | rDCgaaSBAWYfsxUYhCk1n2… | 999.99/XRP |

### Credit Graph



r3kmLJN5D28dHuH8vZNUZpMC43pEHpaocV

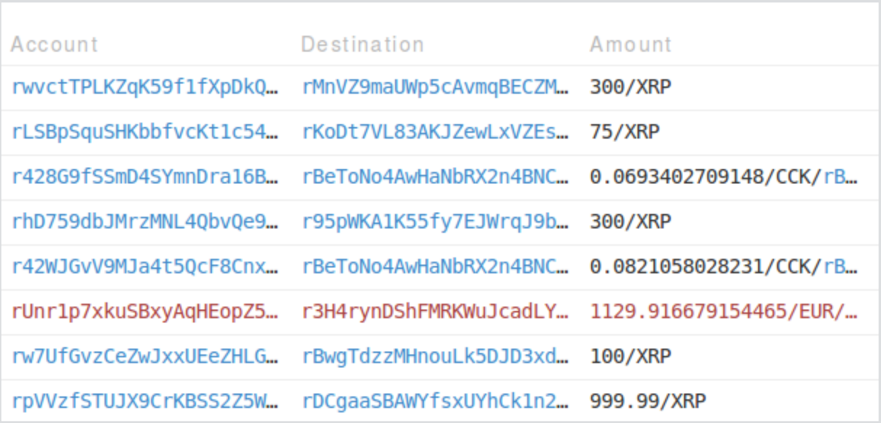
All Currencies

# Public Verifiability & Privacy Problem

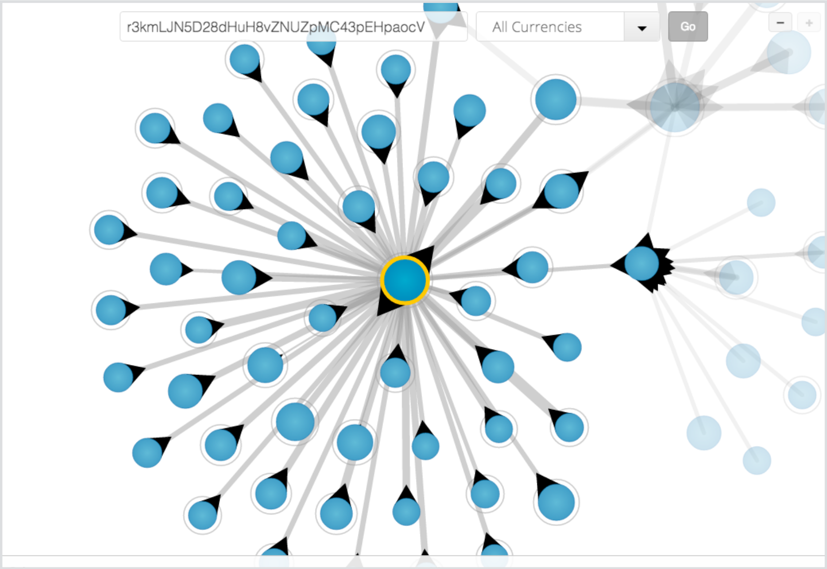
## The Ripple Ledger

### Credit Graph

### Transaction Details



| Account | Destination | Amount |
|---|---|---|
| rwvctTPLKZqK59f1fXpDkQ… | rMnVZ9maUWp5cAvmqBECZM… | 300/XRP |
| rLSBpSquSHKbbfvcKt1c54… | rKoDt7VL83AKJZewLxVZEs… | 75/XRP |
| r428G9fSSmD4SYmnDra16B… | rBeToNo4AwHaNbRX2n4BNC… | 0.0693402709148/CCK/rB… |
| rhD759dbJMrzMNL4QbvQe9… | r95pWKA1K55fy7EJWrqJ9b… | 300/XRP |
| r42WJGvV9MJa4t5QcF8Cnx… | rBeToNo4AwHaNbRX2n4BNC… | 0.0821058028231/CCK/rB… |
| rUnr1p7xkuSBxyAqHEopZ5… | r3H4rynDShFMRKWuJcadLY… | 1129.916679154465/EUR/… |
| rw7UfGvzCeZwJxxUEeZHLG… | rBwgTdzzMHnouLk5DJD3xd… | 100/XRP |
| rpVVzfSTUJX9CrKBSS2Z5W… | rDCgaaSBAWYfsxUYhCk1n2… | 999.99/XRP |



**Listening to Whispers of Ripple: Linking Wallets and Deanonymizing Transactions in the Ripple Network**

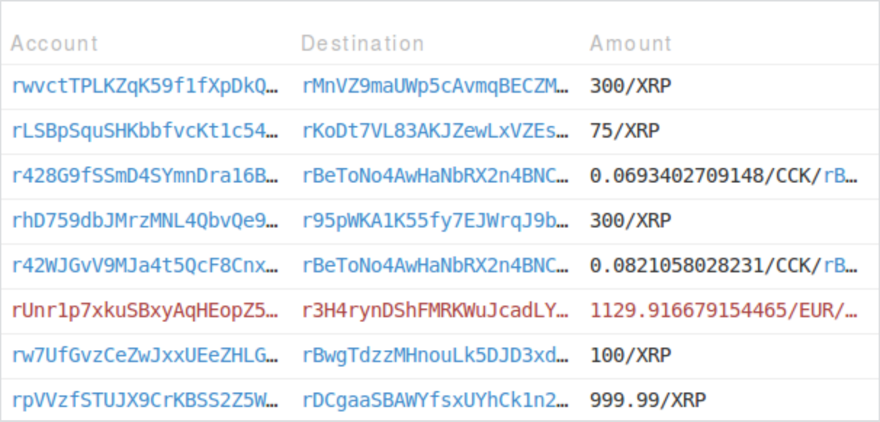
Pedro Moreno-Sanchez, Muhammad Bilal Zafar, Aniket Kate.

PETS '16

# Public Verifiability & Privacy Problem

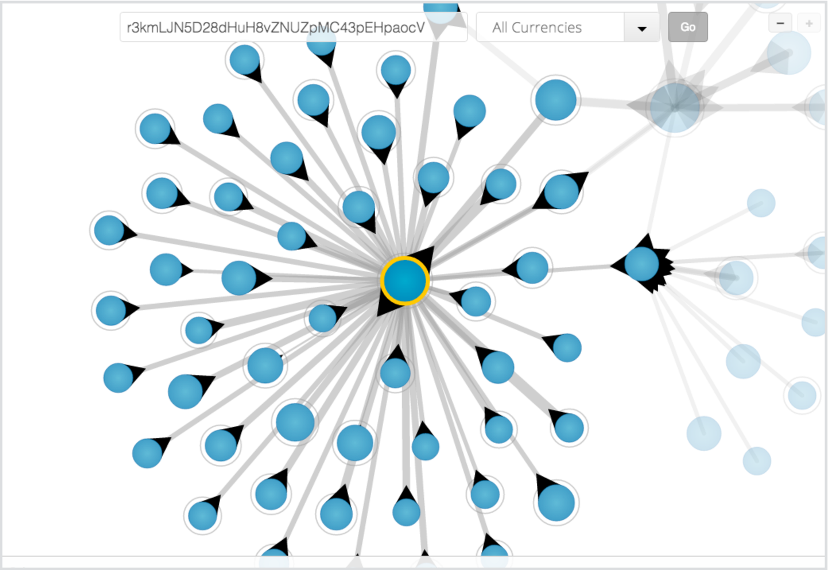
## The Ripple Ledger

### Transaction Details



| Account | Destination | Amount |
|---|---|---|
| rwvctTPLKZqK59f1fXpDkQ… | rMnVZ9maUWp5cAvmqBECZM… | 300/XRP |
| rLSBpSquSHKbbfvcKt1c54… | rKoDt7VL83AKJZewLxVZEs… | 75/XRP |
| r428G9fSSmD4SYmnDra16B… | rBeToNo4AwHaNbRX2n4BNC… | 0.0693402709148/CCK/rB… |
| rhD759dbJMrzMNL4QbvQe9… | r95pWKA1K55fy7EJWrqJ9b… | 300/XRP |
| r42WJGvV9MJa4t5QcF8Cnx… | rBeToNo4AwHaNbRX2n4BNC… | 0.0821058028231/CCK/rB… |
| rUnr1p7xkuSBxyAqHEopZ5… | r3H4rynDShFMRKWuJcadLY… | 1129.916679154465/EUR/… |
| rw7UfGvzCeZwJxxUEeZHLG… | rBwgTdzzMHnouLk5DJD3xd… | 100/XRP |
| rpVVzfSTUJX9CrKBSS2Z5W… | rDCgaaSBAWYfsxUYhCk1n2… | 999.99/XRP |

### Credit Graph



r3kmLJN5D28dHuH8vZNUZpMC43pEHpaocV

All Currencies

**Listening to Whispers of Ripple: Linking Wallets and Deanonymizing Transactions in the Ripple Network**

Pedro Moreno-Sanchez, Muhammad Bilal Zafar, Aniket Kate.

PETS ‘16

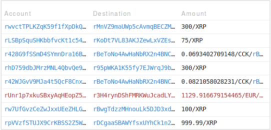
Current credit networks employ a global ledger

# Our Contributions

- We question the need for a global ledger and global consensus

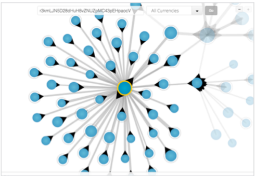
The Ripple Ledger

Transaction Details



| Account | Destination | Amount |
|---|---|---|
| rwvctTPLKZqK59f1fXpDkQ… | rMnVZ9maUWp5cAvmqBECZM… | 300/XRP |
| rLSBpSquSHKbbfvcKt1c54… | rKoDt7VL83AKJZewLxVZEs… | 75/XRP |
| r428G9fSSmD4SYmnDra16B… | rBeToNo4AwHaNbRX2n4BNC… | 0.0693402709148/CCK/rB… |
| rhD759dbJMrzMNL4QbvQe9… | r95pWKA1K55fy7EJWrqJ9b… | 300/XRP |
| r42WJGvV9MJa4t5QcF8Cnx… | rBeToNo4AwHaNbRX2n4BNC… | 0.0821058028231/CCK/rB… |
| rUnr1p7xkuSBxyAqHEopZ5… | r3H4rynDShFMRKWuJcadLY… | 1129.916679154465/EUR/… |
| rw7UfGvzCeZwJxxUEeZHLG… | rBwgTdzzMHnouLk5DJD3xd… | 100/XRP |
| rpVVzfSTUJX9CrKBSS2Z5W… | rDCgaaSBAWYfsxUYhCk1n2… | 999.99/XRP |

Credit Graph

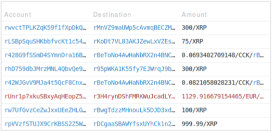


# Our Contributions

- We question the need for a global ledger and global consensus

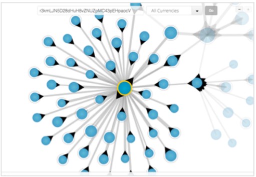
The Ripple Ledger

Transaction Details



| Account | Destination | Amount |
|---|---|---|
| rwvctTPLKZqK59f1fXpDkQ… | rMnVZ9maUWp5cAvmqBECZM… | 300/XRP |
| rLSBpSquSHKbbfvcKt1c54… | rKoDt7VL83AKJZewLxVZEs… | 75/XRP |
| r428G9fSSmD4SYmnDra16B… | rBeToNo4AwHaNbRX2n4BNC… | 0.0693402709148/CCK/rB… |
| rhD759dbJMrzMNL4QbvQe9… | r95pWKA1K55fy7EJWrqJ9b… | 300/XRP |
| r42WJGvV9MJa4t5QcF8Cnx… | rBeToNo4AwHaNbRX2n4BNC… | 0.0821058028231/CCK/rB… |
| rUnr1p7xkuSBxyAqHEopZ5… | r3H4rynDShFMRKWuJcadLY… | 1129.916679154465/EUR/… |
| rw7UfGvzCeZwJxxUEeZHLG… | rBwgTdzzMHnouLk5DJD3xd… | 100/XRP |
| rpVVzfSTUJX9CrKBSS2Z5W… | rDCgaaSBAWYfsxUYhCk1n2… | 999.99/XRP |

Credit Graph

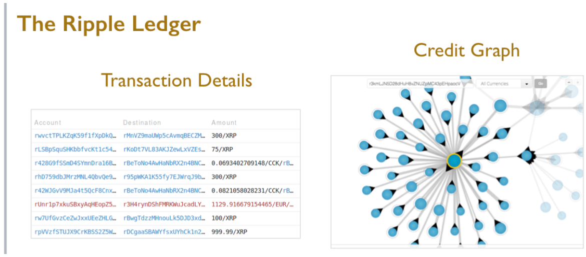


- SilentWhispers: Decentralized credit network with security and privacy guarantees defined in UC framework

**Inspired by our work in NDSS’15**

# Our Contributions

- We question the need for a global ledger and global consensus



The Ripple Ledger

Transaction Details

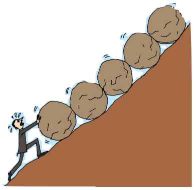
| Account | Destination | Amount |
|---|---|---|
| rwvctTPLKZqK59f1fXpDkQ… | rMnVZ9maUWp5cAvmqBECZM… | 300/XRP |
| rLSBpSquSHKbbfvcKt1c54… | rKoDt7VL83AKJZewLxVZEs… | 75/XRP |
| r428G9fSSmD4SYmnDra16B… | rBeToNo4AwHaNbRX2n4BNC… | 0.0693402709148/CCK/rB… |
| rhD759dbJMrzMNL4QbvQe9… | r95pWKA1K55fy7EJWrqJ9b… | 300/XRP |
| r42WJGvV9MJa4t5QcF8Cnx… | rBeToNo4AwHaNbRX2n4BNC… | 0.0821058028231/CCK/rB… |
| rUnr1p7xkuSBxyAqHEopZ5… | r3H4rynDShFMRKWuJcadLY… | 1129.916679154465/EUR/… |
| rw7UfGvzCeZwJxxUEeZHLG… | rBwgTdzzMHnouLk5DJD3xd… | 100/XRP |
| rpVVzfSTUJX9CrKBSS2Z5W… | rDCgaaSBAWYfsxUYhCk1n2… | 999.99/XRP |

Credit Graph

- SilentWhispers: Decentralized credit network with security and privacy guarantees defined in UC framework

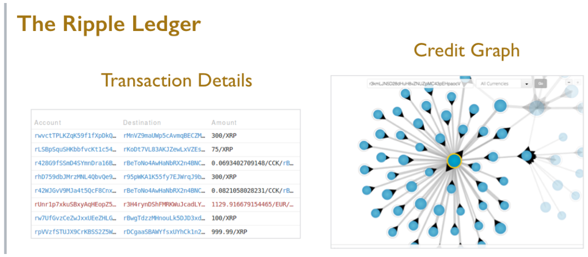
**Inspired by our work in NDSS'15**

- SilentWhispers overcomes several challenges: existence of a path, credit on a path and integrity of transactions



# Our Contributions

- We question the need for a global ledger and global consensus



The Ripple Ledger

Transaction Details

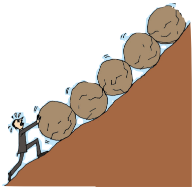
| Account | Destination | Amount |
|---|---|---|
| rwvctTPLKZqK59f1fXpDkQ… | rMnVZ9maUWp5cAvmqBECZM… | 300/XRP |
| rLSBpSquSHKbbfvcKt1c54… | rKoDt7VL83AKJZewLxVZEs… | 75/XRP |
| r428G9fSSmD4SYmnDra16B… | rBeToNo4AwHaNbRX2n4BNC… | 0.0693402709148/CCK/rB… |
| rhD759dbJMrzMNL4QbvQe9… | r95pWKA1K55fy7EJWrqJ9b… | 300/XRP |
| r42WJGvV9MJa4t5QcF8Cnx… | rBeToNo4AwHaNbRX2n4BNC… | 0.0821058028231/CCK/rB… |
| rUnr1p7xkuSBxyAqHEopZ5… | r3H4rynDShFMRKWuJcadLY… | 1129.916679154465/EUR/… |
| rw7UfGvzCeZwJxxUEeZHLG… | rBwgTdzzMHnouLk5DJD3xd… | 100/XRP |
| rpVVzfSTUJX9CrKBSS2Z5W… | rDCgaaSBAWYfsxUYhCk1n2… | 999.99/XRP |

Credit Graph

- SilentWhispers: Decentralized credit network with security and privacy guarantees defined in UC framework

**Inspired by our work in NDSS’15**

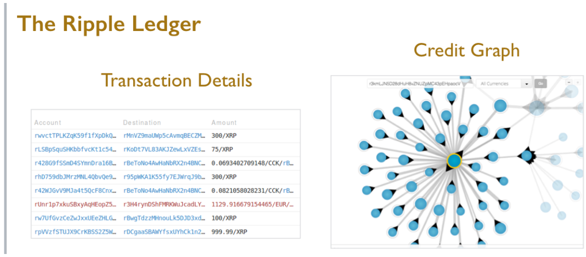
- SilentWhispers overcomes several challenges: existence of a path, credit on a path and integrity of transactions



- SilentWhispers uses distributed landmark routing, secure multi-party computation and 2-step transactions

# Our Contributions

- ✦ We question the need for a global ledger and global consensus



The Ripple Ledger

Transaction Details

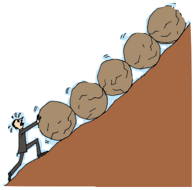
| Account | Destination | Amount |
|---|---|---|
| rwvctTPLKZqK59f1fXpDkQ… | rMnVZ9maUWp5cAvmqBECZM… | 300/XRP |
| rLSBpSquSHKbbfvcKt1c54… | rKoDt7VL83AKJZewLxVZEs… | 75/XRP |
| r428G9fSSmD4SYmnDra16B… | rBeToNo4AwHaNbRX2n4BNC… | 0.0693402709148/CCK/rB… |
| rhD759dbJMrzMNL4QbvQe9… | r95pWKA1K55fy7EJWrqJ9b… | 300/XRP |
| r42WJGvV9MJa4t5QcF8Cnx… | rBeToNo4AwHaNbRX2n4BNC… | 0.0821058028231/CCK/rB… |
| rUnr1p7xkuSBxyAqHEopZ5… | r3H4rynDShFMRKWuJcadLY… | 1129.916679154465/EUR/… |
| rw7UfGvzCeZwJxxUEeZHLG… | rBwgTdzzMHnouLk5DJD3xd… | 100/XRP |
| rpVVzfSTUJX9CrKBSS2Z5W… | rDCgaaSBAWYfsxUYhCk1n2… | 999.99/XRP |

Credit Graph

- ✦ SilentWhispers: Decentralized credit network with security and privacy guarantees defined in UC framework

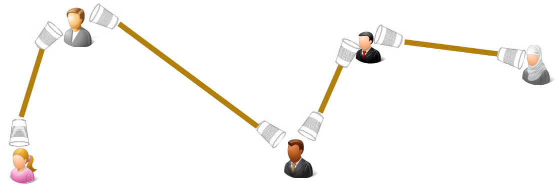
**Inspired by our work in NDSS'15**

- ✦ SilentWhispers overcomes several challenges: existence of a path, credit on a path and integrity of transactions



- ✦ SilentWhispers uses distributed landmark routing, secure multi-party computation and 2-step transactions

- ✦ SilentWhispers is feasible in practice and offers interesting alternatives to current emerging payment systems



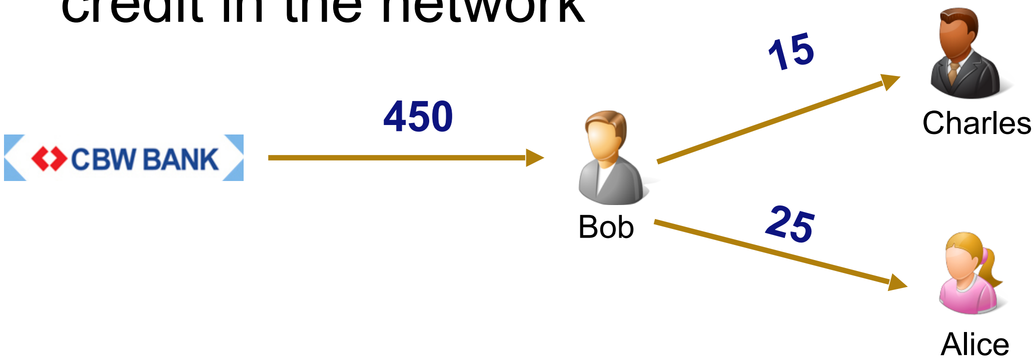
# SilentWhispers: A Decentralized Credit Network

# SilentWhispers: A Decentralized Credit Network

- Local Information suffices: Credit links of a user determine his credit in the network

# SilentWhispers: A Decentralized Credit Network

- Local Information suffices: Credit links of a user determine his credit in the network

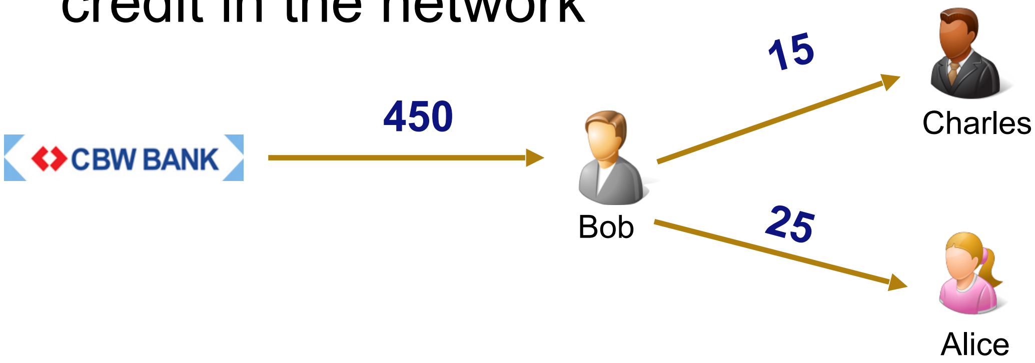


In-flow = 450
Out-flow = 40

Net-flow = 410

# SilentWhispers: A Decentralized Credit Network

- Local Information suffices: Credit links of a user determine his credit in the network



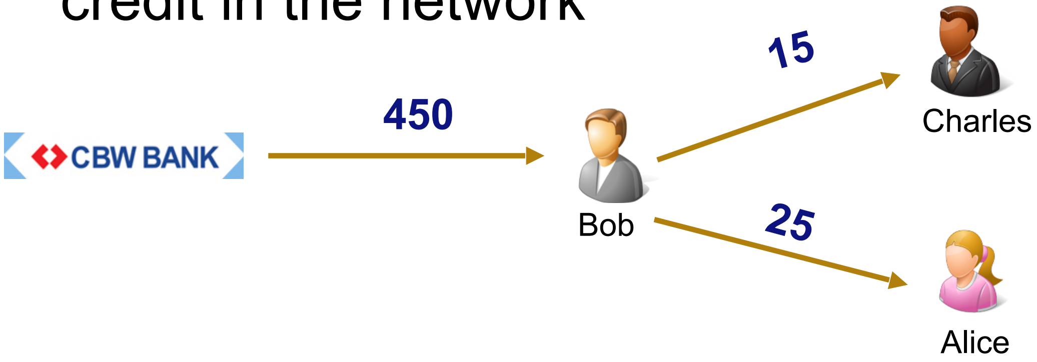
In-flow = 450
Out-flow = 40

Net-flow = 410

- Net-flow is what matters: Net-flow of a user must not change without the user's consent

# SilentWhispers: A Decentralized Credit Network

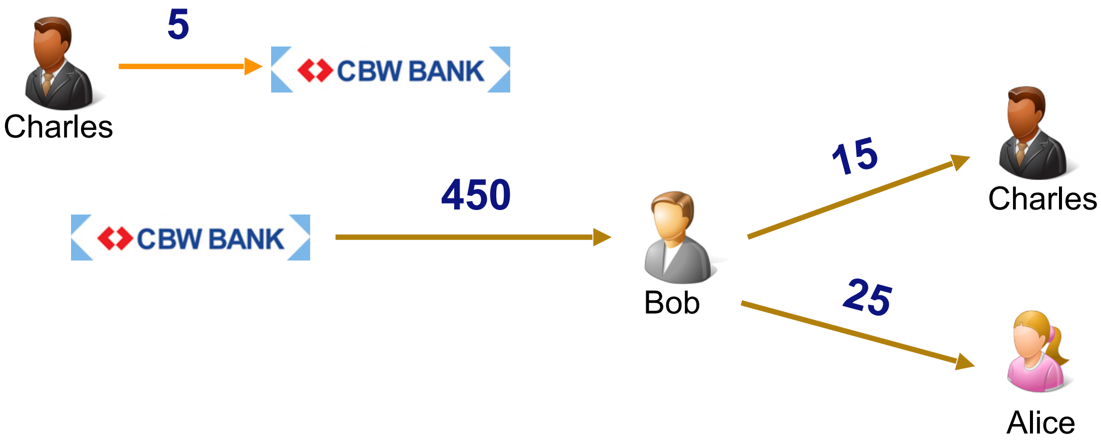
- Local Information suffices: Credit links of a user determine his credit in the network



In-flow = 450
Out-flow = 40

Net-flow = 410

- Net-flow is what matters: Net-flow of a user must not change without the user's consent

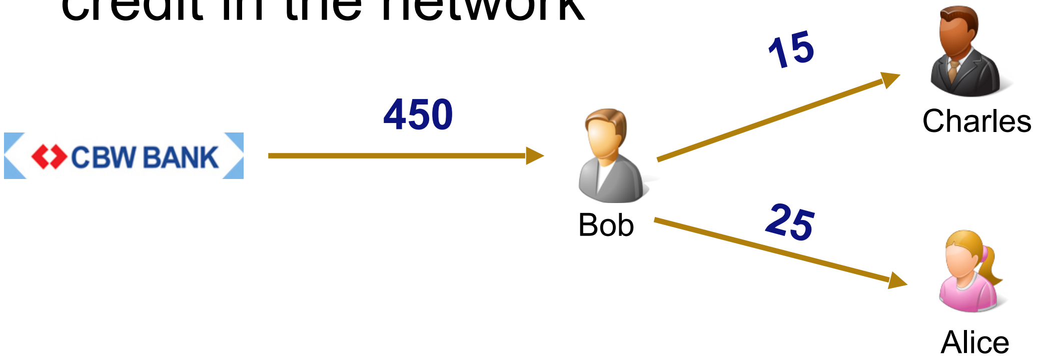


In-flow = 450
Out-flow = 40

Net-flow = 410

# SilentWhispers: A Decentralized Credit Network

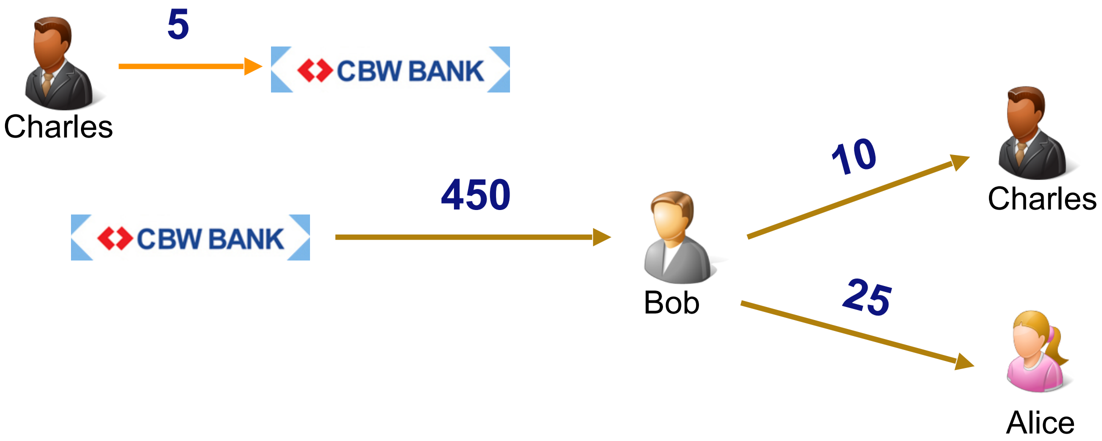
- Local Information suffices: Credit links of a user determine his credit in the network



In-flow = 450
Out-flow = 40

Net-flow = 410

- Net-flow is what matters: Net-flow of a user must not change without the user's consent

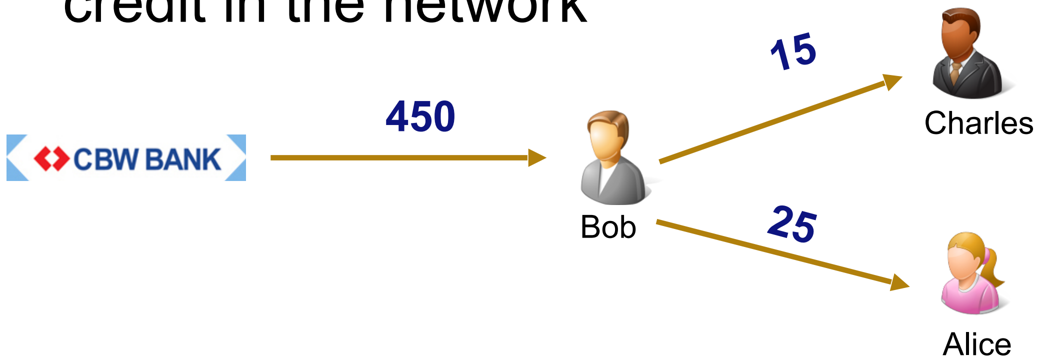


In-flow = 450
Out-flow = 40

Net-flow = 410

# SilentWhispers: A Decentralized Credit Network

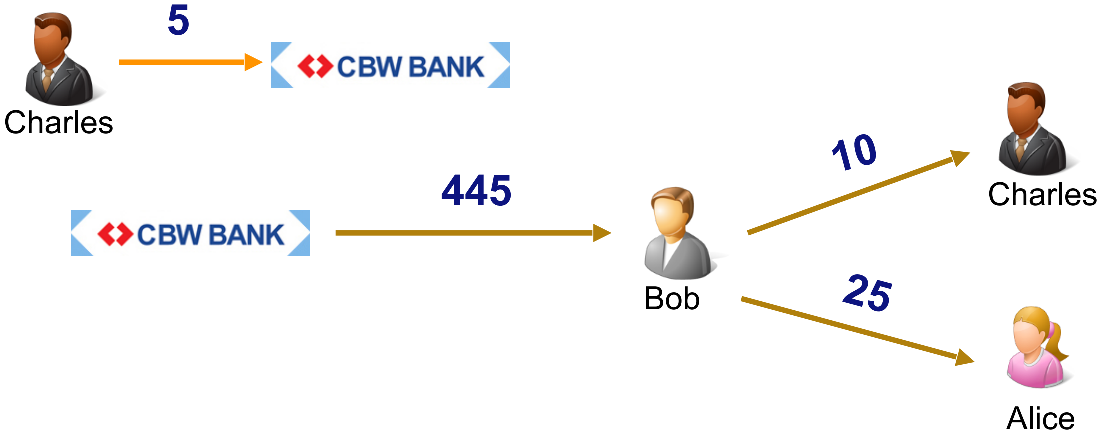
- Local Information suffices: Credit links of a user determine his credit in the network



In-flow = 450
Out-flow = 40

Net-flow = 410

- Net-flow is what matters: Net-flow of a user must not change without the user's consent

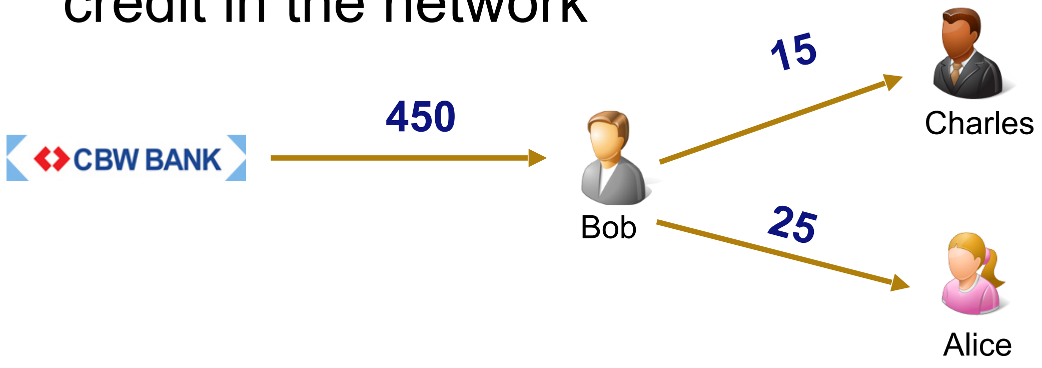


In-flow = 450
Out-flow = 40

Net-flow = 410

# SilentWhispers: A Decentralized Credit Network

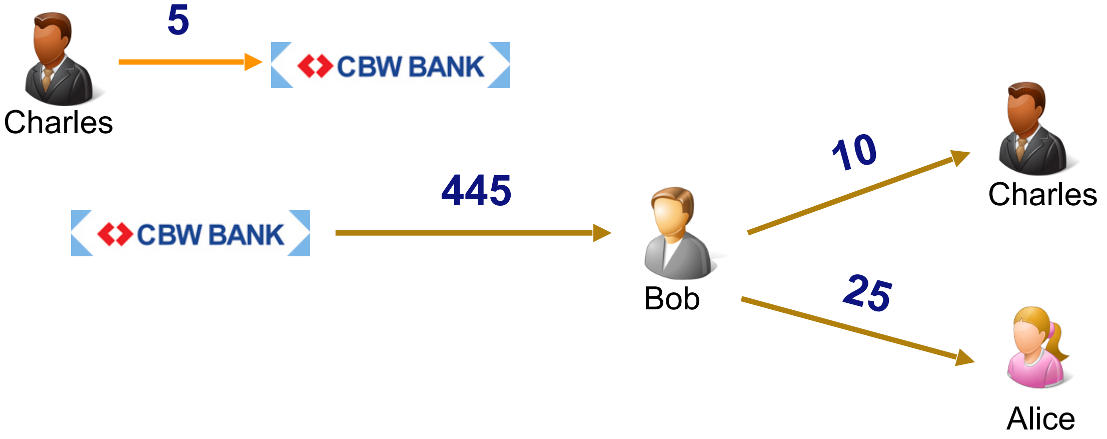
- Local Information suffices: Credit links of a user determine his credit in the network



In-flow = 450
Out-flow = 40

Net-flow = 410

- Net-flow is what matters: Net-flow of a user must not change without the user's consent

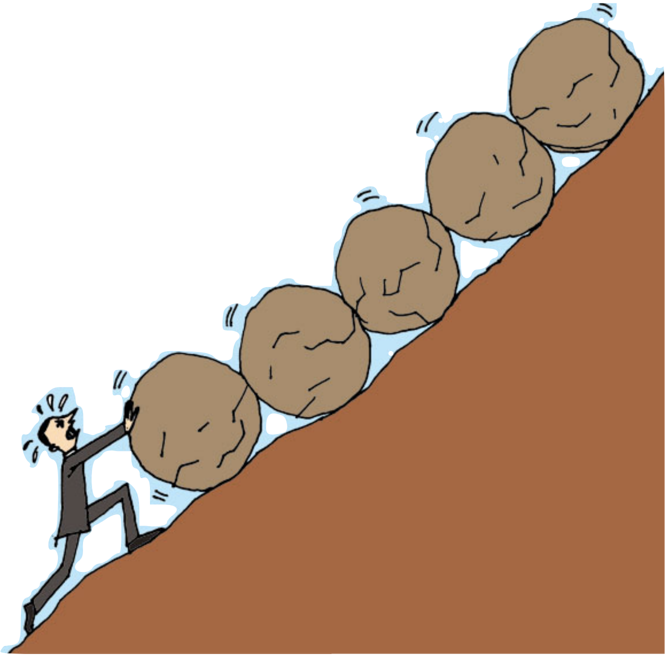


In-flow = ~~450~~ 445
Out-flow = ~~40~~ 35

Net-flow = 410

# Challenges

- Find paths between users
- Calculate credit available in the path
- Ensure integrity of transactions
- And more …



# The routing challenge

# Routing Challenge: Landmark Routing

# Routing Challenge: Landmark Routing

- Determine credit path from sender to receiver

# Routing Challenge: Landmark Routing

- Determine credit path from sender to receiver
- Common problem in standard networks and ad-hoc networks

# Routing Challenge: Landmark Routing

- Determine credit path from sender to receiver
- Common problem in standard networks and ad-hoc networks
- The max-flow approach:
  - Not scalable enough: $O(V^3)$ or $O(V^2 log(E))$

# Routing Challenge: Landmark Routing

- Determine credit path from sender to receiver
- Common problem in standard networks and ad-hoc networks
- The max-flow approach:
  - Not scalable enough: $O(V^3)$ or $O(V^2 log(E))$
- Landmark routing [Tschusiya ’89]
  - Calculate subset of all paths

# Routing Challenge: Landmark Routing

- Determine credit path from sender to receiver

- Common problem in standard networks and ad-hoc networks

- The max-flow approach:
  - Not scalable enough: $O(V^3)$ or $O(V^2 log(E))$

- Landmark routing [Tschusiya ’89]
  - Calculate subset of all paths

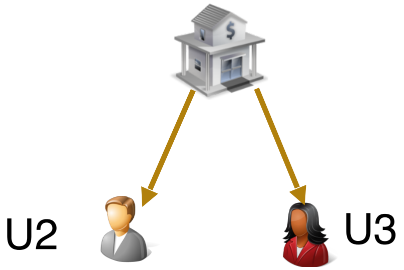
# Routing Challenge: Landmark Routing

- Determine credit path from sender to receiver

- Common problem in standard networks and ad-hoc networks

- The max-flow approach:
  - Not scalable enough: $O(V^3)$ or $O(V^2 log(E))$

- Landmark routing [Tschusiya ’89]
  - Calculate subset of all paths



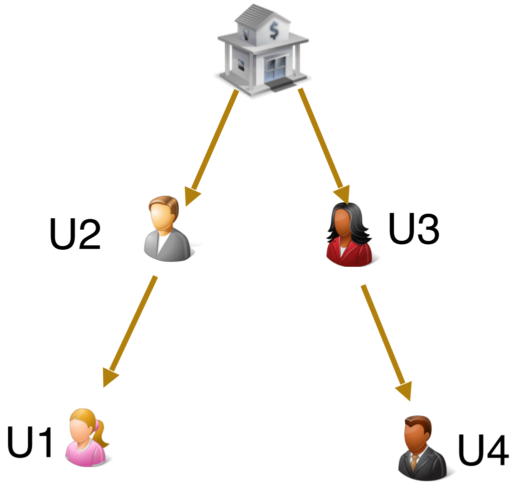
# Routing Challenge: Landmark Routing

- Determine credit path from sender to receiver

- Common problem in standard networks and ad-hoc networks

- The max-flow approach:
  - Not scalable enough: $O(V^3)$ or $O(V^2 log(E))$

- Landmark routing [Tschusiya ’89]
  - Calculate subset of all paths



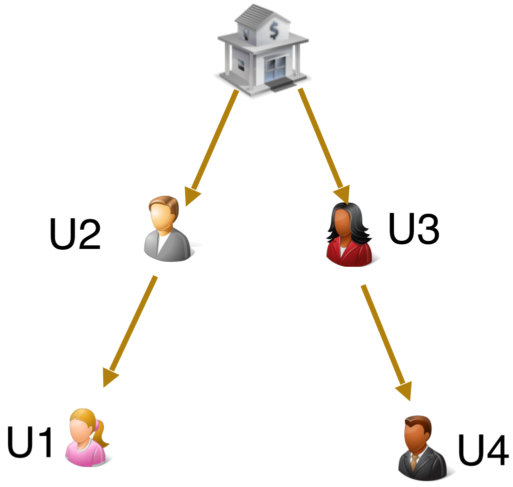
# Routing Challenge: Landmark Routing

- Determine credit path from sender to receiver

- Common problem in standard networks and ad-hoc networks

- The max-flow approach:
  - Not scalable enough: $O(V^3)$ or $O(V^2 log(E))$

- Landmark routing [Tschusiya ’89]
  - Calculate subset of all paths
  - Distributed BFS: Local information suffices



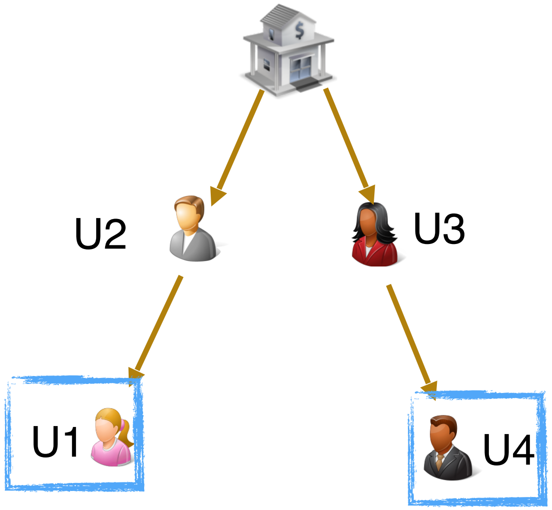
# Routing Challenge: Landmark Routing

- Determine credit path from sender to receiver

- Common problem in standard networks and ad-hoc networks

- The max-flow approach:
  - Not scalable enough: *$O(V^3)$* or *$O(V^2 log(E))$*

- Landmark routing [Tschusiya ’89]
  - Calculate subset of all paths
  - Distributed BFS: Local information suffices



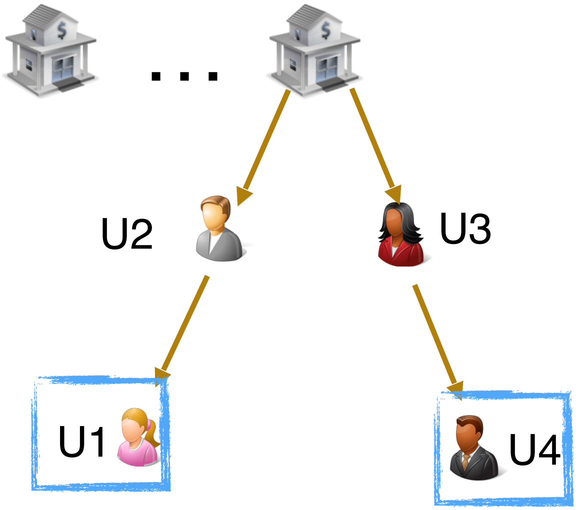
# Routing Challenge: Landmark Routing

- Determine credit path from sender to receiver

- Common problem in standard networks and ad-hoc networks

- The max-flow approach:
  - Not scalable enough: $O(V^3)$ or $O(V^2 log(E))$

- Landmark routing [Tschusiya ’89]
  - Calculate subset of all paths
  - Distributed BFS: Local information suffices



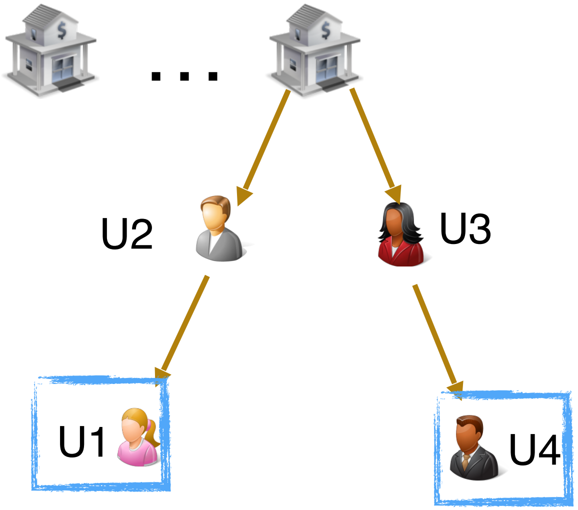
# Routing Challenge: Landmark Routing

- Determine credit path from sender to receiver

- Common problem in standard networks and ad-hoc networks

- The max-flow approach:
  - Not scalable enough: $O(V^3)$ or $O(V^2 log(E))$

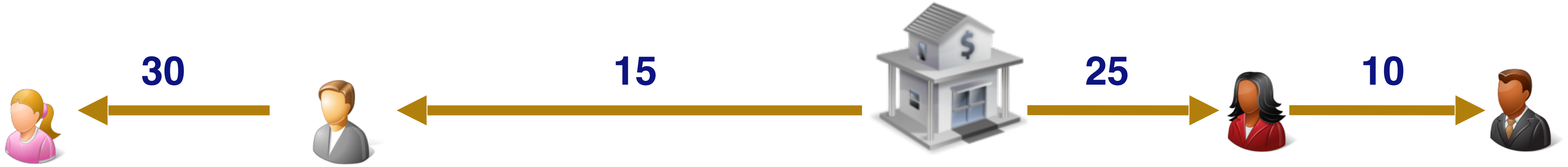
- Landmark routing [Tschusiya ’89]
  - Calculate subset of all paths
  - Distributed BFS: Local information suffices
  - Enough in practice[1,2]
  - More efficient than max-flow[1,2]



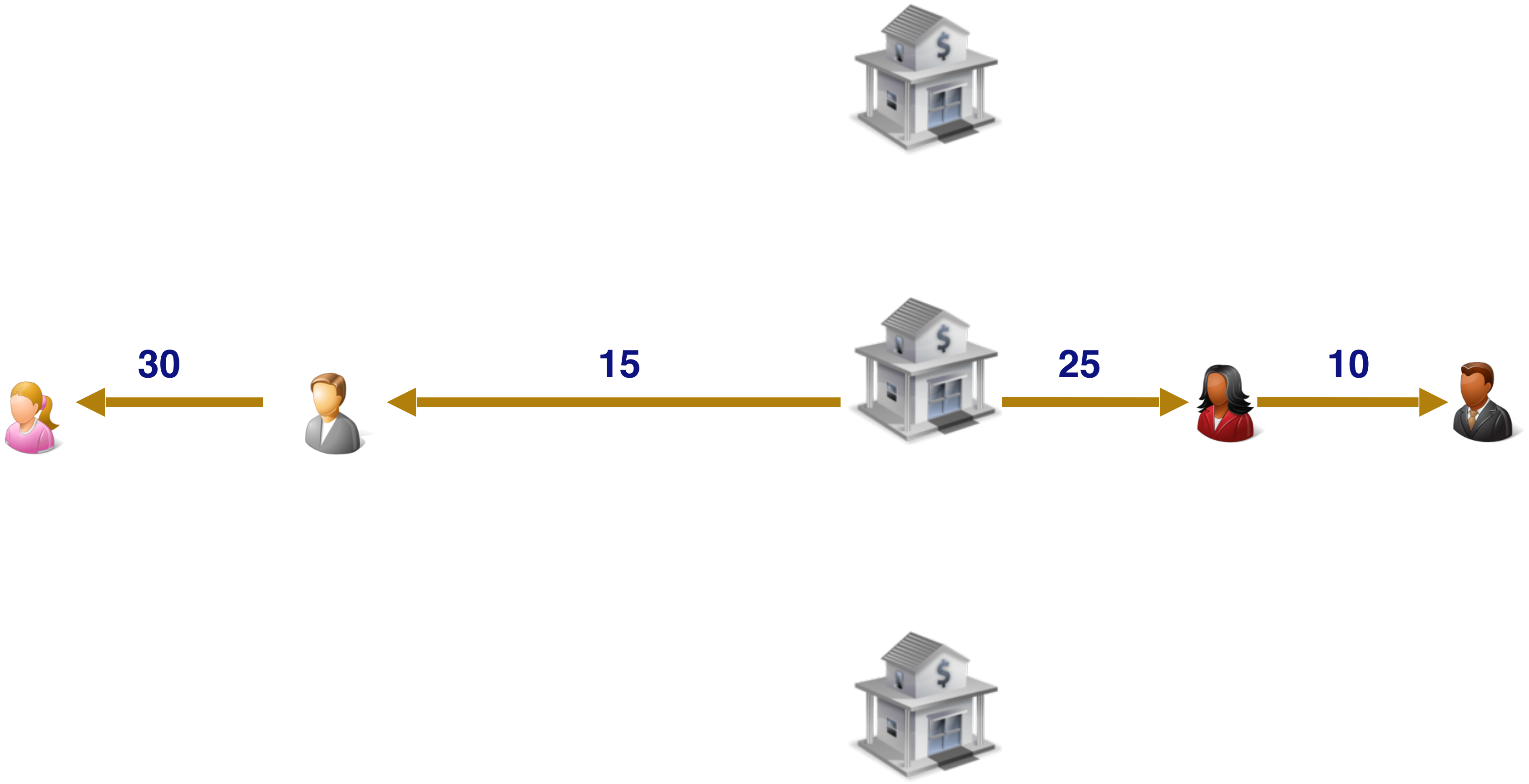
[1] [Our work in NDSS ’15]
[2] [Viswanath et al. EUROSYS ’12]

# Calculation of credit available in a path

# Credit in a Path: SMPC

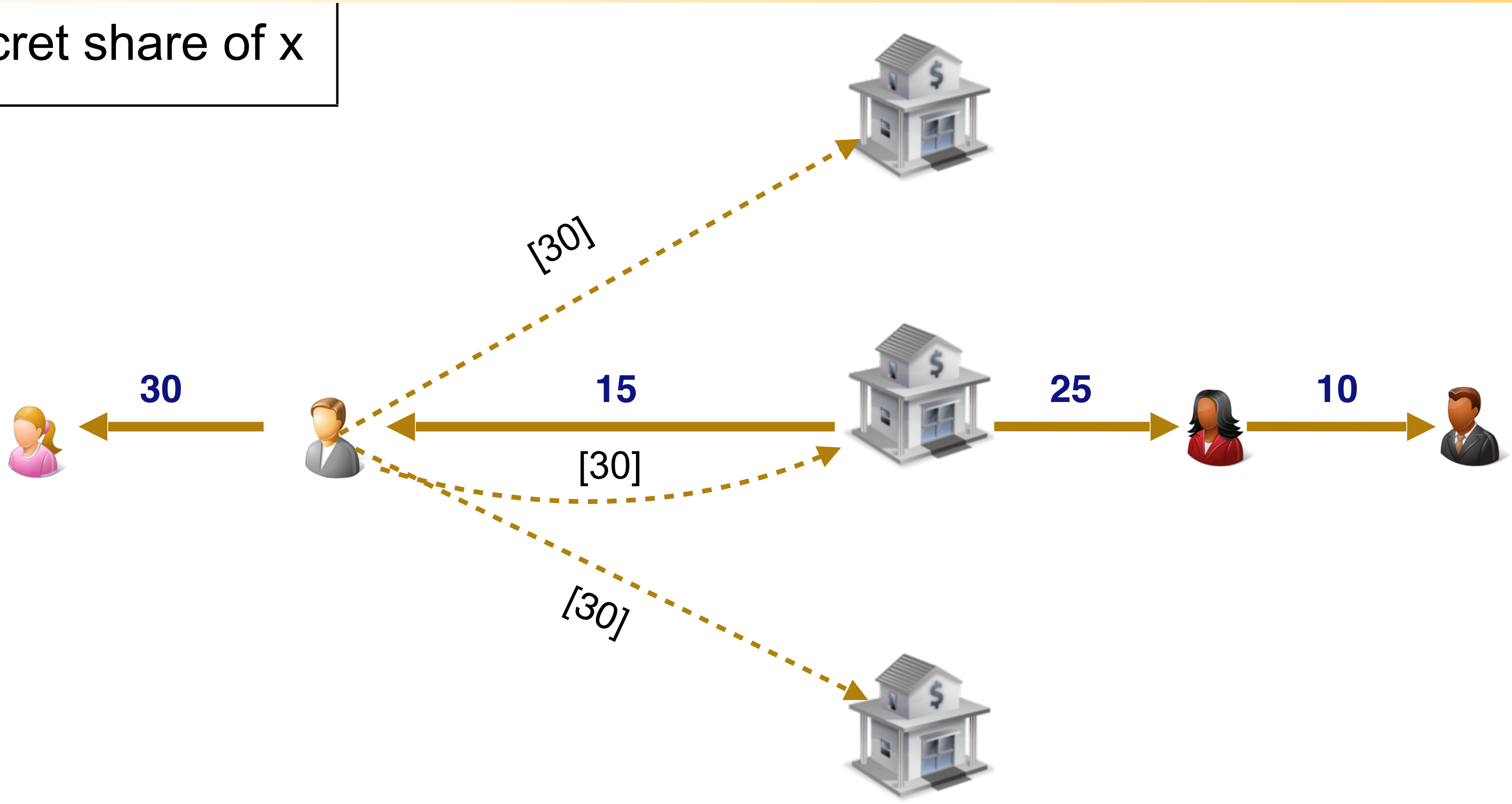


# Credit in a Path: SMPC



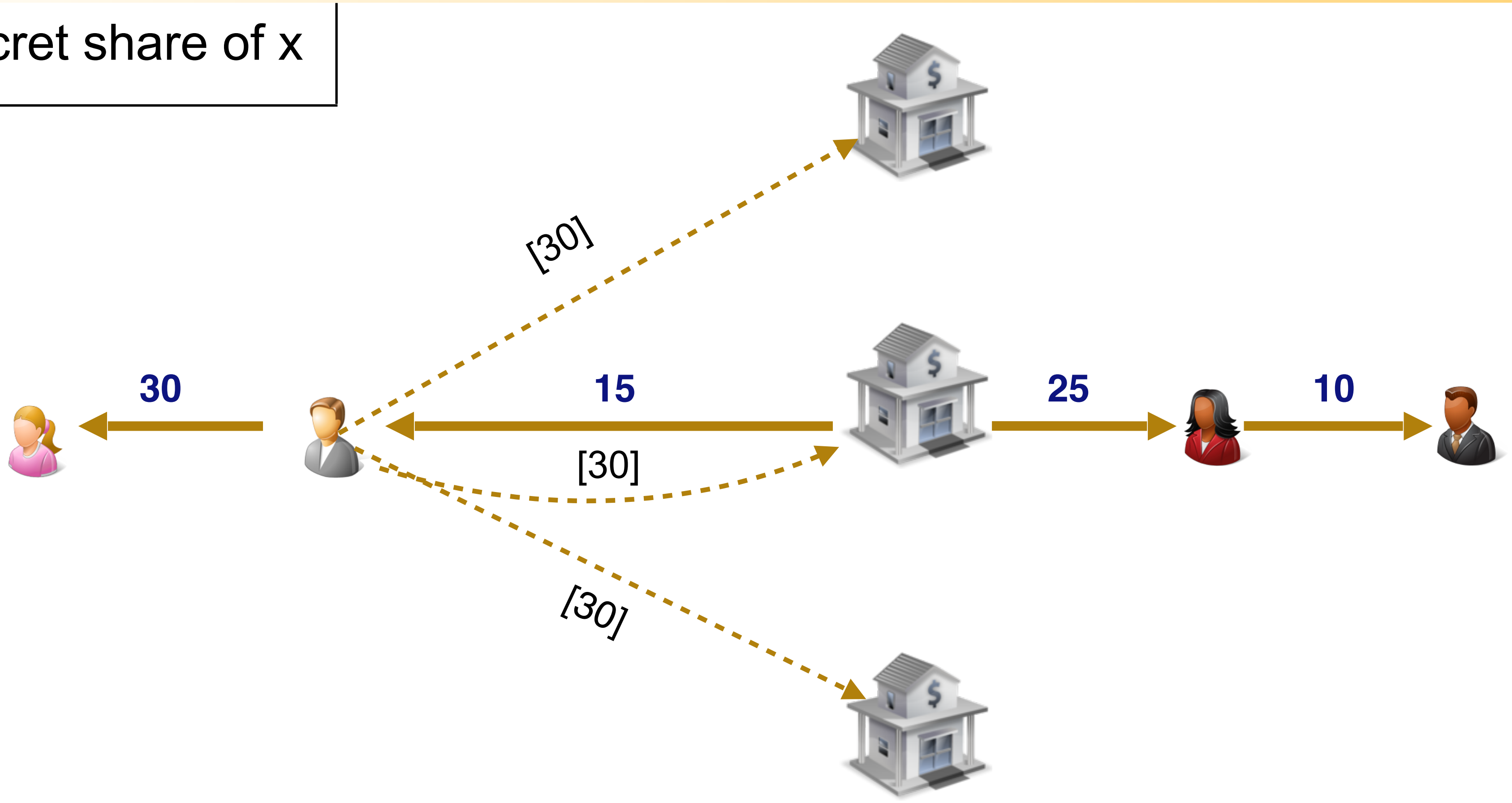
# Credit in a Path: SMPC

[x]: Secret share of x



# Credit in a Path: SMPC

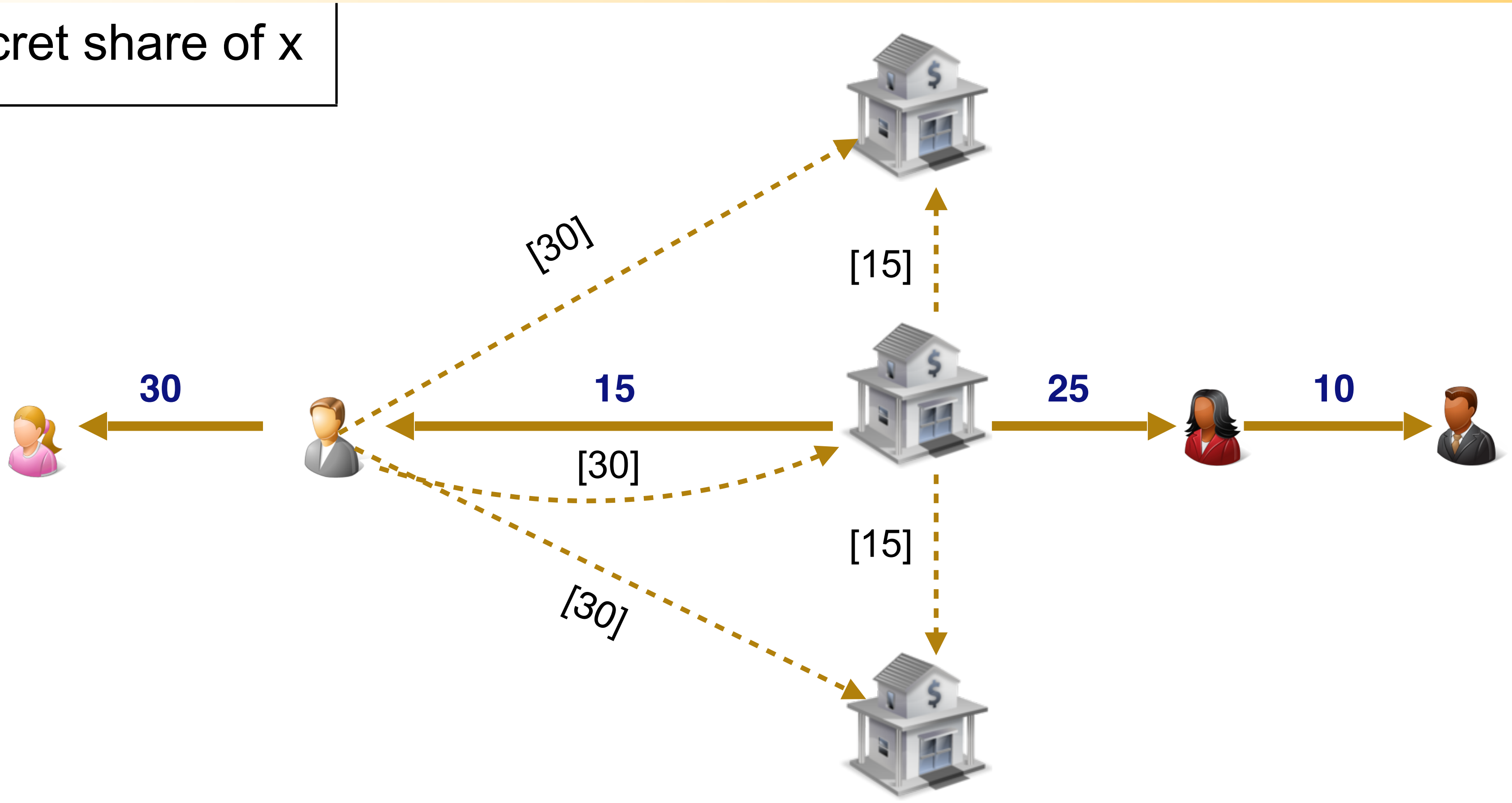
[x]: Secret share of x



- Given [x] it is not possible to know x

# Credit in a Path: SMPC

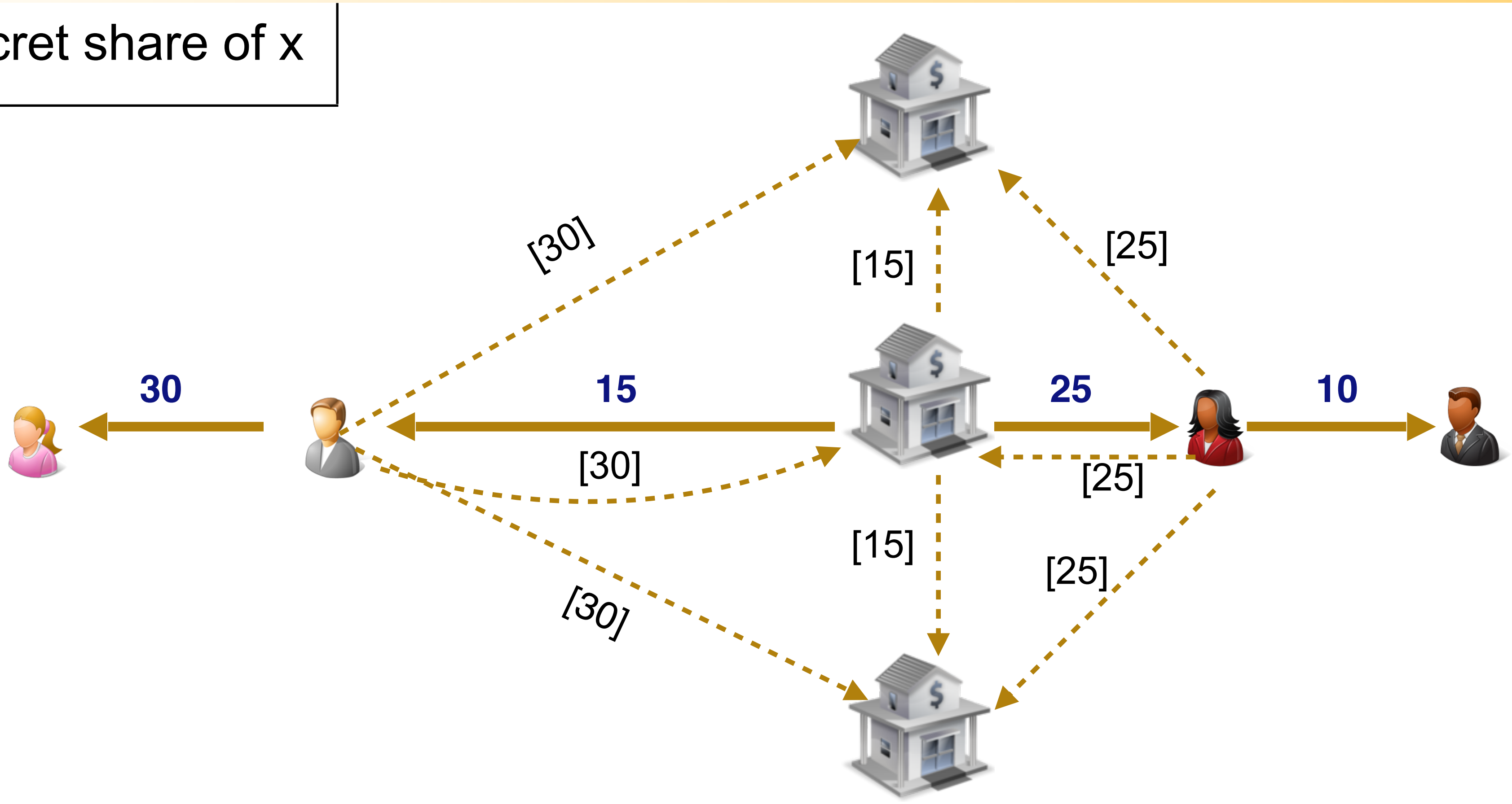
[x]: Secret share of x



- Given [x] it is not possible to know x

# Credit in a Path: SMPC

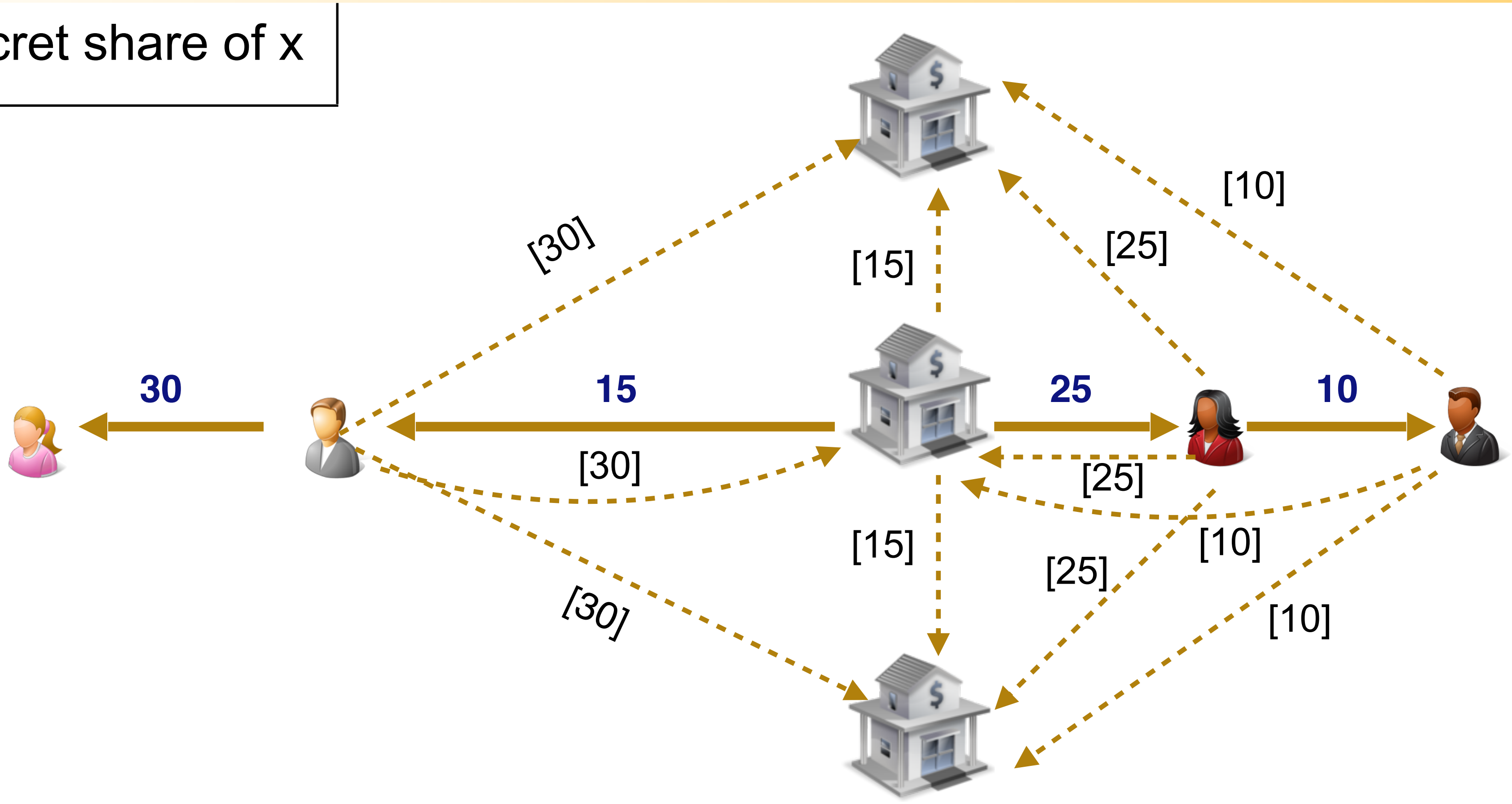
[x]: Secret share of x



- Given [x] it is not possible to know x

# Credit in a Path: SMPC

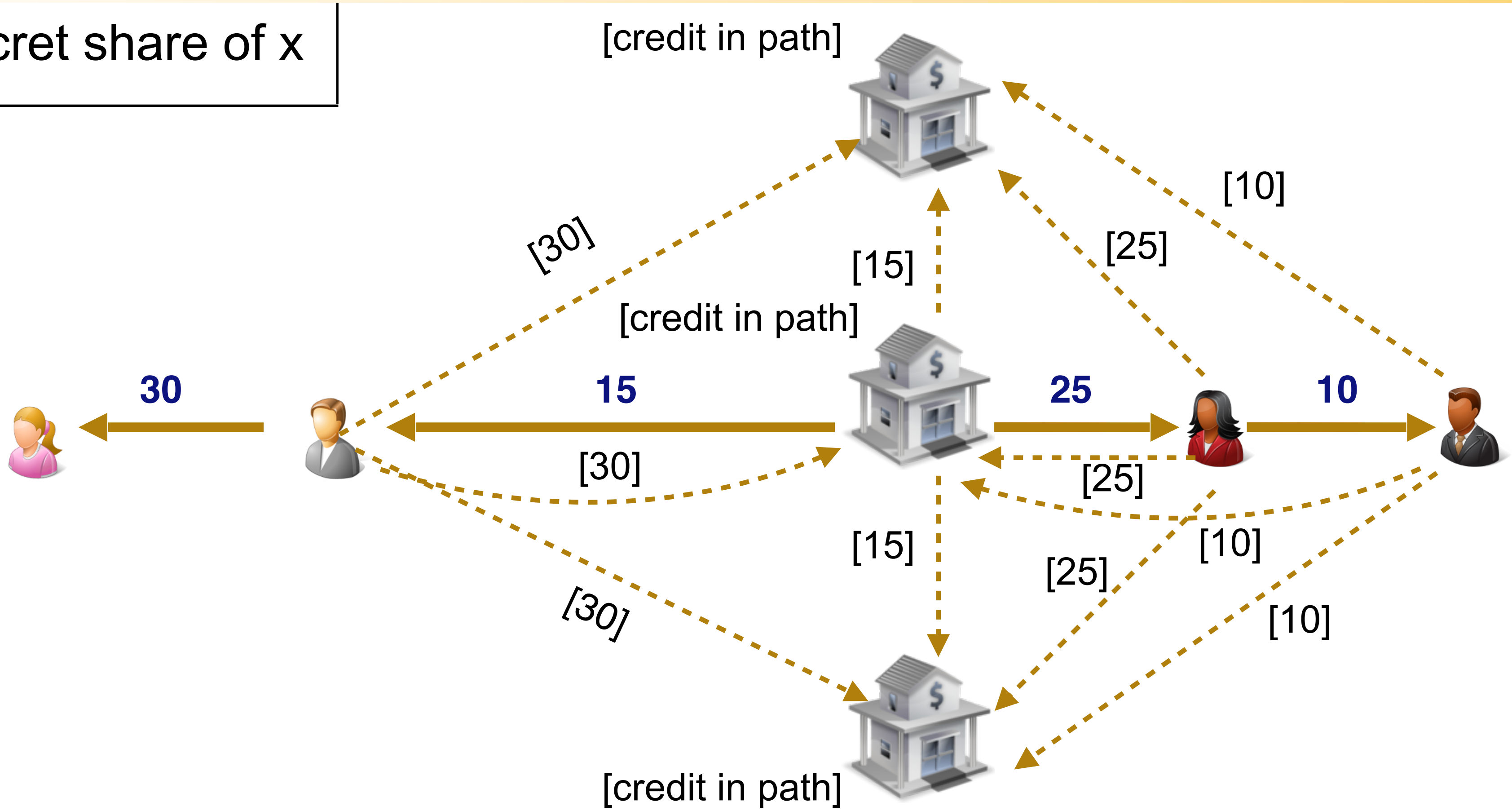
[x]: Secret share of x



- Given [x] it is not possible to know x

# Credit in a Path: SMPC

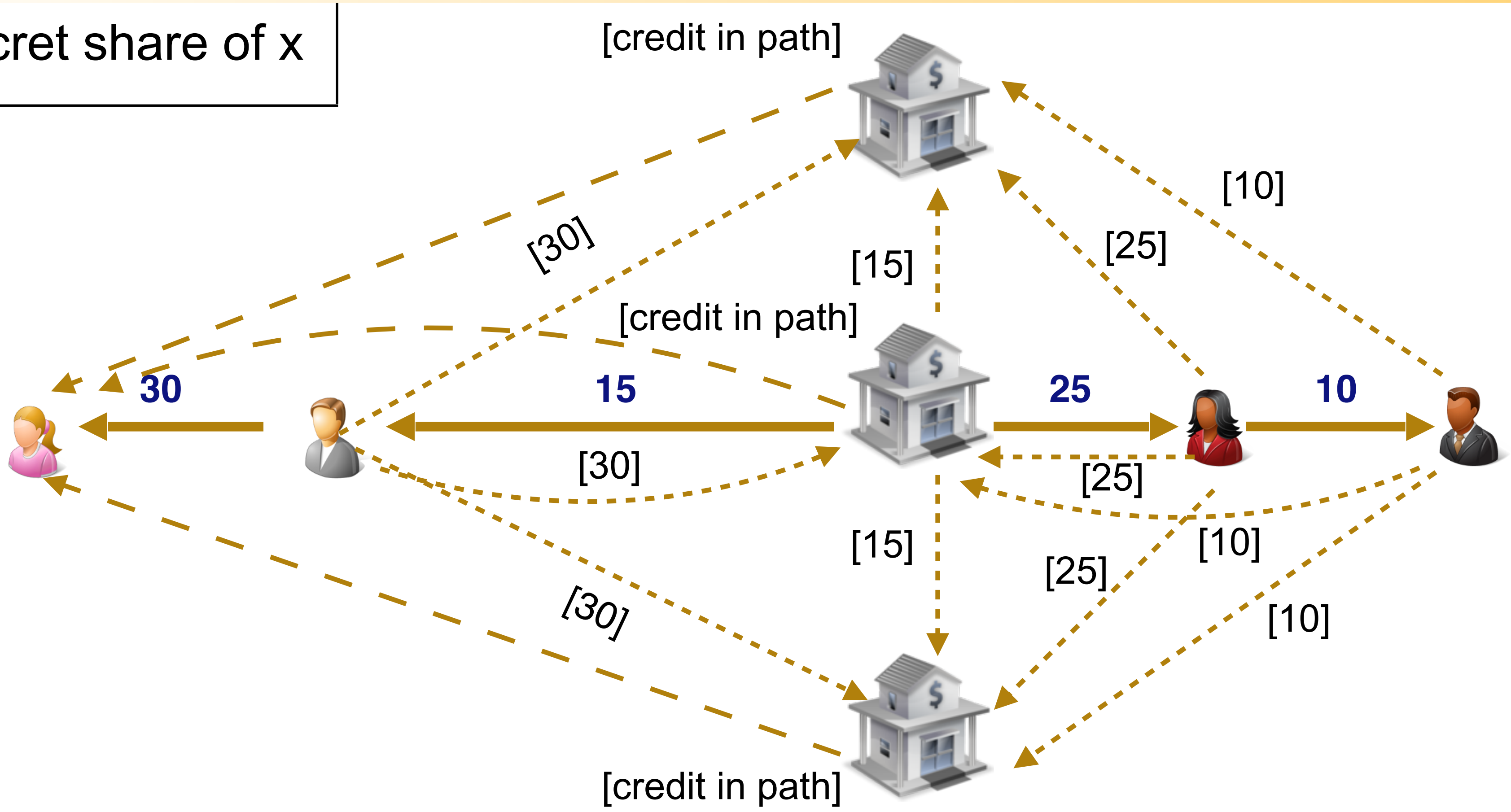
[x]: Secret share of x



- Given [x] it is not possible to know x

# Credit in a Path: SMPC

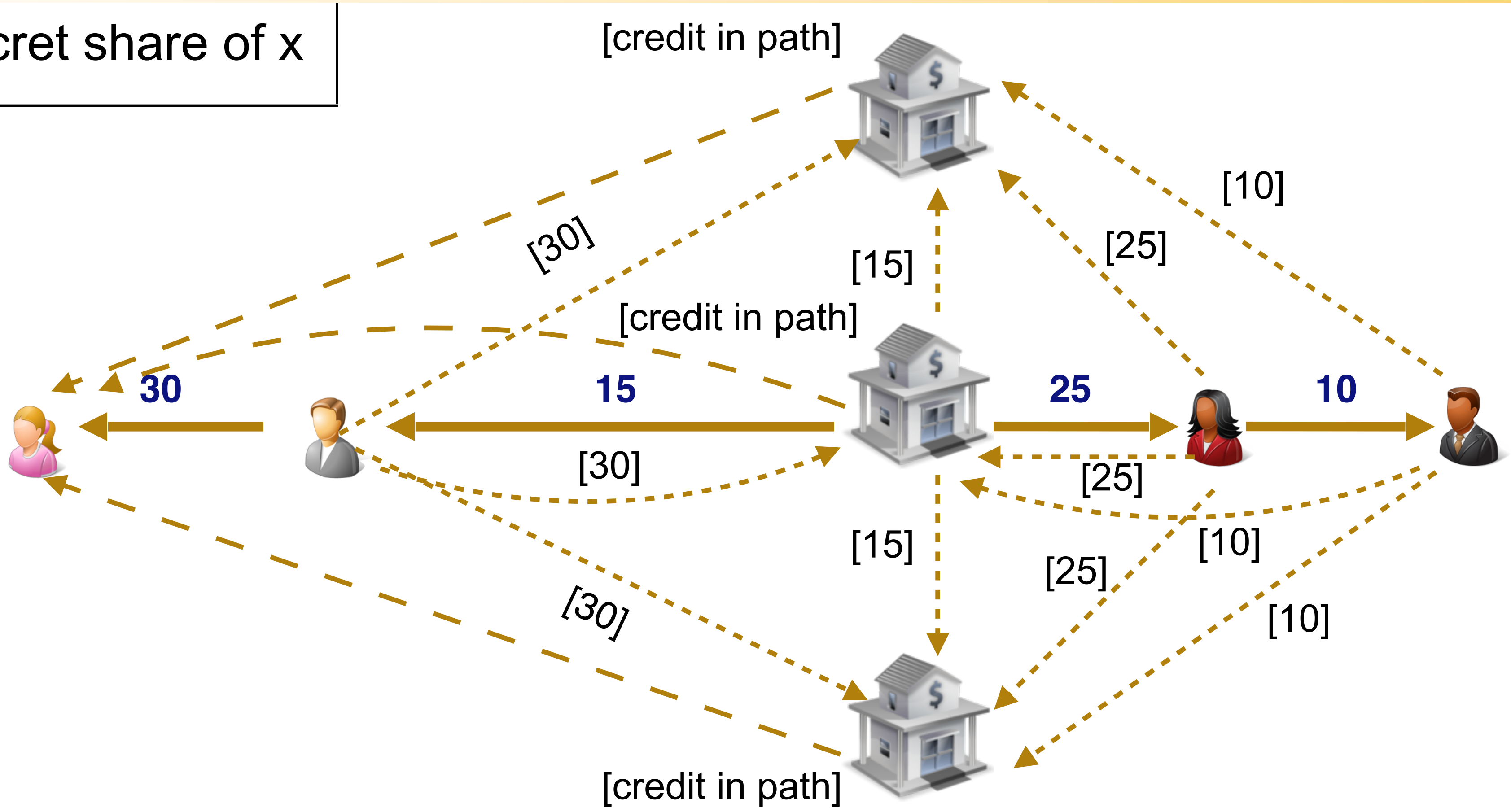
[x]: Secret share of x



- Given [x] it is not possible to know x

# Credit in a Path: SMPC

[x]: Secret share of x



- Given [x] it is not possible to know x
  - Given “enough” copies of [x] one can reconstruct x

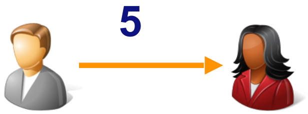
# Integrity of the transactions

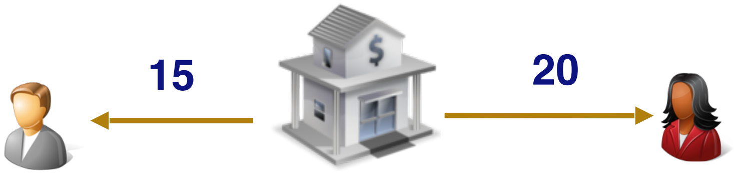
# Transaction Integrity and Dispute Resolution

# Transaction Integrity and Dispute Resolution

- 2-step transaction: on hold and settle

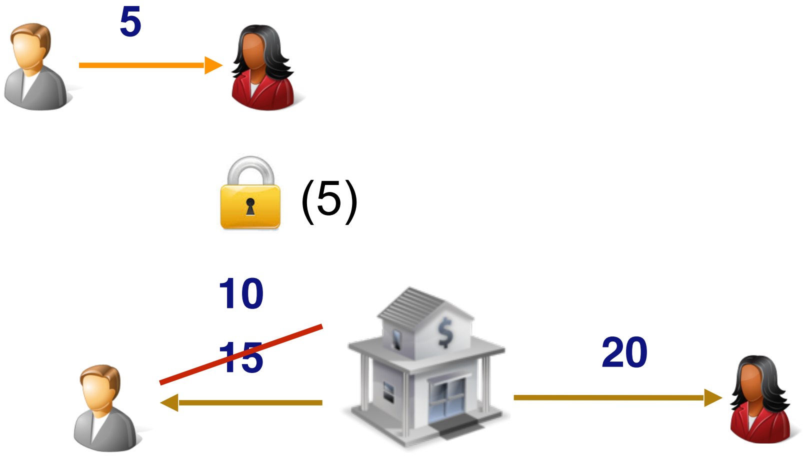
# Transaction Integrity and Dispute Resolution

- 2-step transaction: on hold and settle
- Example: 



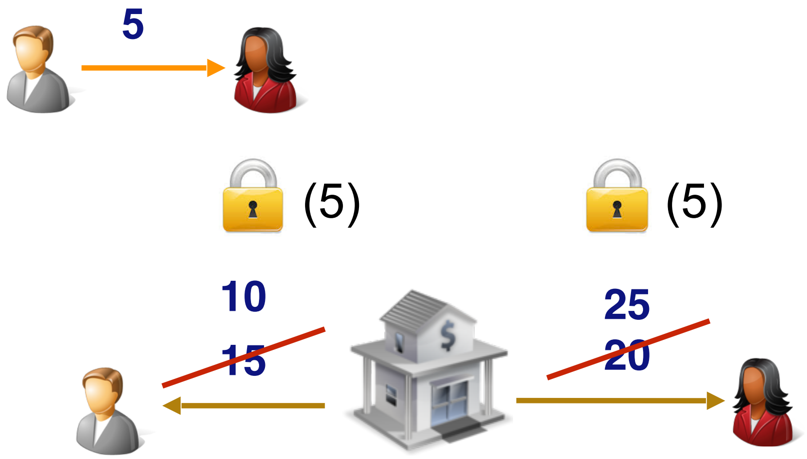
# Transaction Integrity and Dispute Resolution

- 2-step transaction: on hold and settle
- Example:



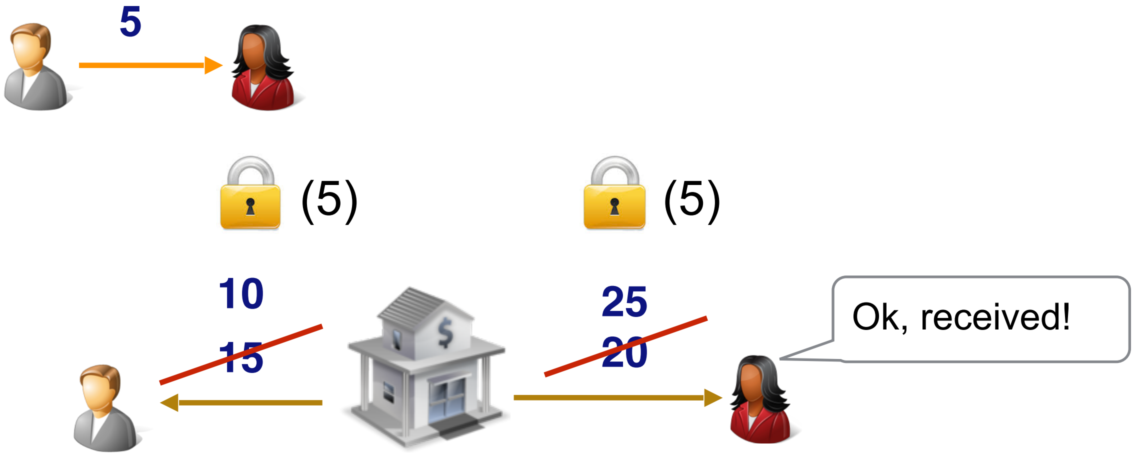
# Transaction Integrity and Dispute Resolution

- 2-step transaction: on hold and settle
- Example:



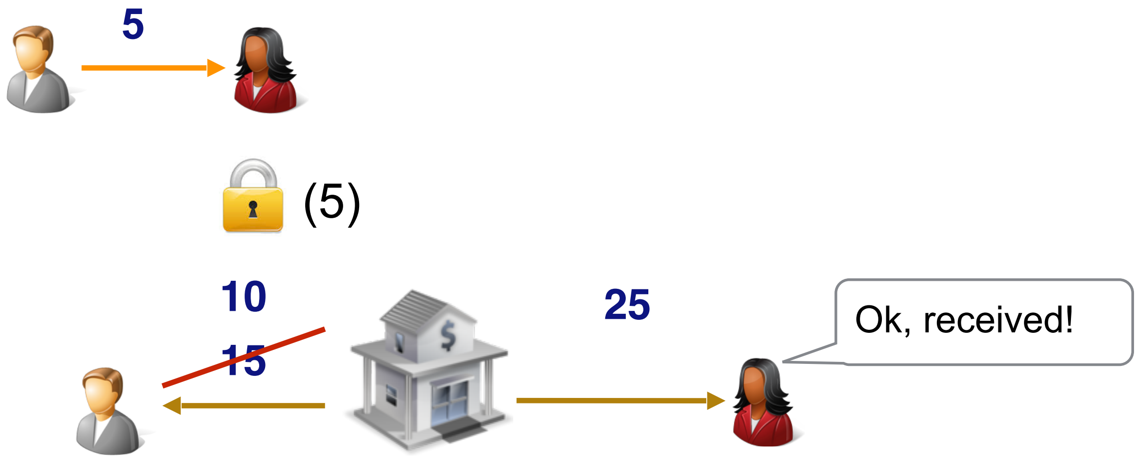
# Transaction Integrity and Dispute Resolution

- 2-step transaction: on hold and settle
- Example:



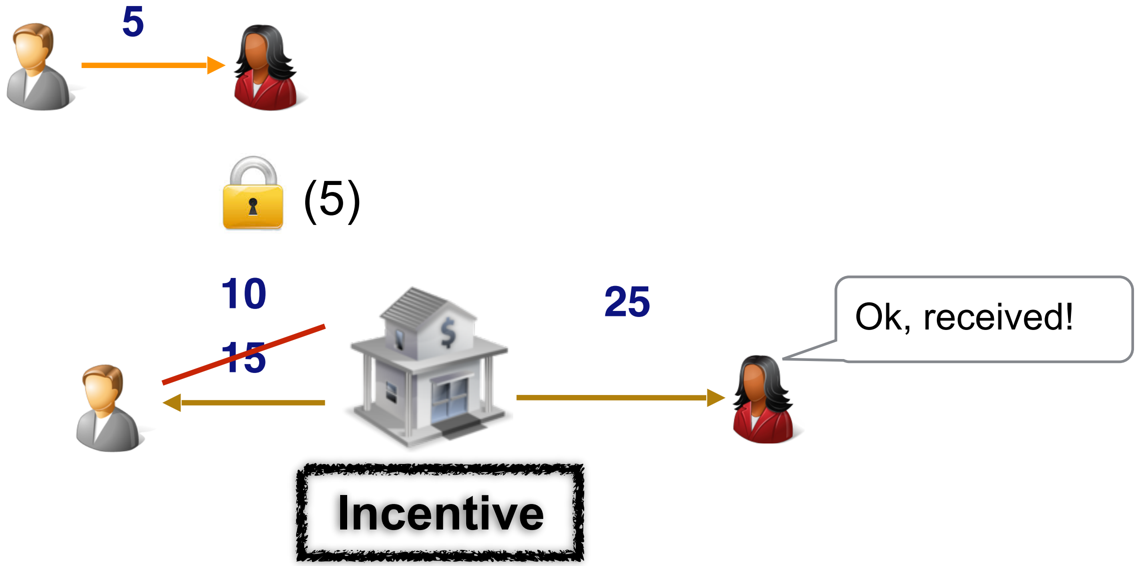
# Transaction Integrity and Dispute Resolution

- 2-step transaction: on hold and settle
- Example:



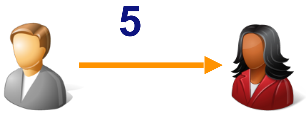
# Transaction Integrity and Dispute Resolution

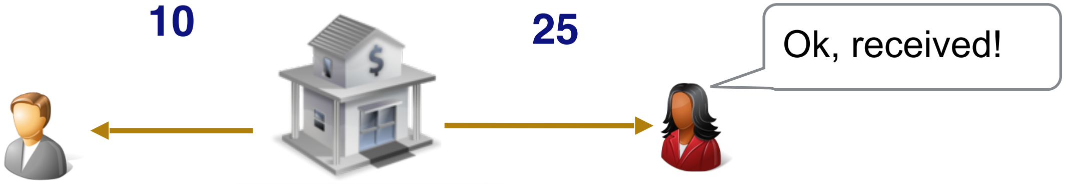
- 2-step transaction: on hold and settle
- Example:



# Transaction Integrity and Dispute Resolution

- 2-step transaction: on hold and settle
- Example:

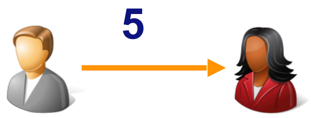


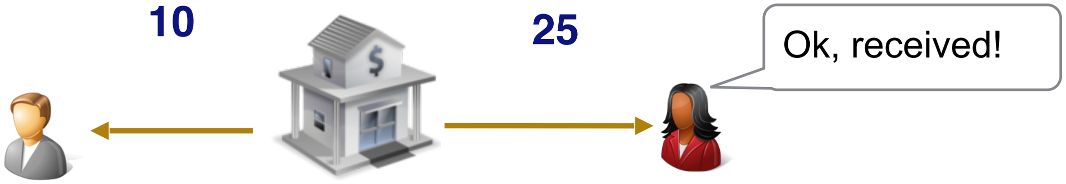


**Incentive**

# Transaction Integrity and Dispute Resolution

- 2-step transaction: on hold and settle
- Example:



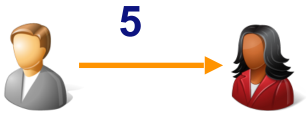


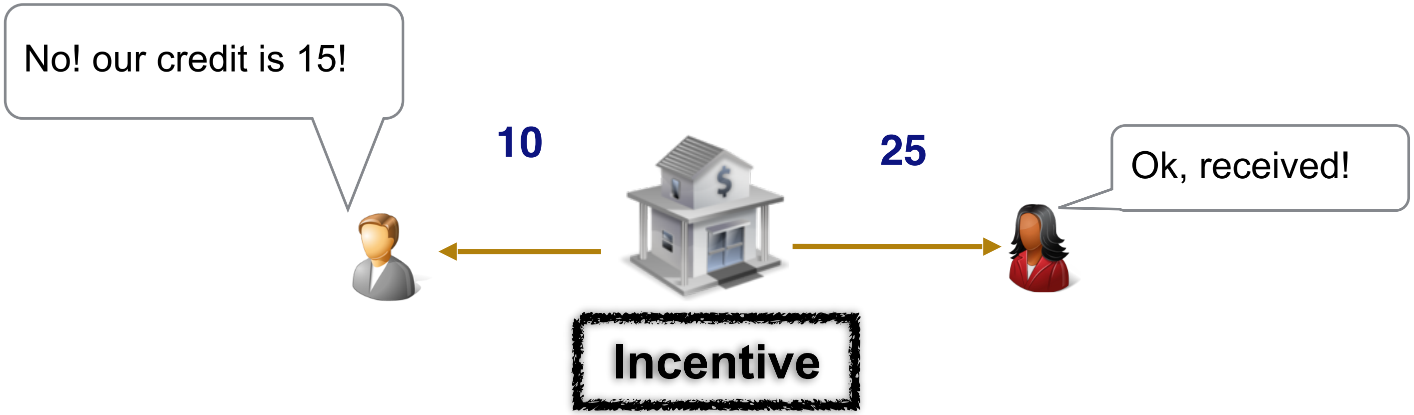
**Incentive**

- Integrity:
  - All landmarks cannot make the user lose credit

# Transaction Integrity and Dispute Resolution

- 2-step transaction: on hold and settle
- Example:




No! our credit is 15!

10

25

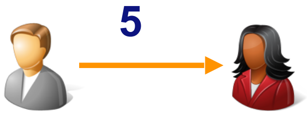
Ok, received!

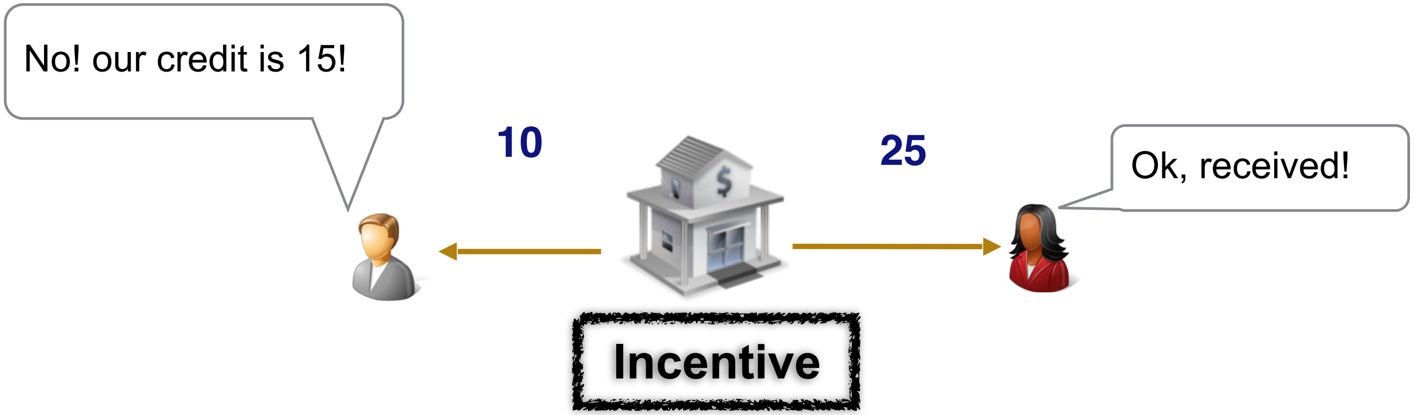
Incentive

- Integrity:
  - All landmarks cannot make the user lose credit

# Transaction Integrity and Dispute Resolution

- 2-step transaction: on hold and settle
- Example:





Incentive

- Integrity:
  - All landmarks cannot make the user lose credit
- Accountability:
  - In case of dispute, users must prove the link value
  - Local logs suffice to determine the valid current value
  - The disputed value is bounded

# Evaluation

# Evaluation and Discussion

# Evaluation and Discussion

- C++ prototype implementation
  - Secret Sharing-based MPC library: https://github.com/Zayat/MPC-Shared

# Evaluation and Discussion

- C++ prototype implementation
  - Secret Sharing-based MPC library: https://github.com/Zayat/MPC-Shared

- Setup using Ripple transactions:
  - Maximum path length: 10 links
  - Maximum number of paths: 7 landmarks (Ripple Gateways)

# Evaluation and Discussion

- C++ prototype implementation
  - Secret Sharing-based MPC library: https://github.com/Zayat/MPC-Shared

- Setup using Ripple transactions:
  - Maximum path length: 10 links
  - Maximum number of paths: 7 landmarks (Ripple Gateways)

- Computing available credit on a path in ~1.3 seconds
  - Different paths in parallel

# Evaluation and Discussion

- C++ prototype implementation
  - Secret Sharing-based MPC library: https://github.com/Zayat/MPC-Shared
- Setup using Ripple transactions:
  - Maximum path length: 10 links
  - Maximum number of paths: 7 landmarks (Ripple Gateways)
- Computing available credit on a path in ~1.3 seconds
  - Different paths in parallel

**Feasible to run in practice current Ripple transactions**

# Evaluation and Discussion

- C++ prototype implementation
  - Secret Sharing-based MPC library: https://github.com/Zayat/MPC-Shared
- Setup using Ripple transactions:
  - Maximum path length: 10 links
  - Maximum number of paths: 7 landmarks (Ripple Gateways)
- Computing available credit on a path in ~1.3 seconds
  - Different paths in parallel

**Feasible to run in practice current Ripple transactions**

- SilentWhispers has attracted attention from industry:
  - KOINA: https://koina.cc/

# The Landscape of Emerging Payment Systems

# The Landscape of Emerging Payment Systems

| | Cryptocurrencies | Ripple | SilentWhispers |
|---|---|---|---|
| **Transfer of funds** | Direct transactions between any two wallets | Transactions only via a path with enough credit | |

# The Landscape of Emerging Payment Systems

| | Cryptocurrencies | Ripple | SilentWhispers |
|---|---|---|---|
| **Transfer of funds** | Direct transactions between any two wallets | Transactions only via a path with enough credit | |
| **Transaction flexibility** | Fixed currency agreed between sender and receiver | Support for cross-currency transactions | |

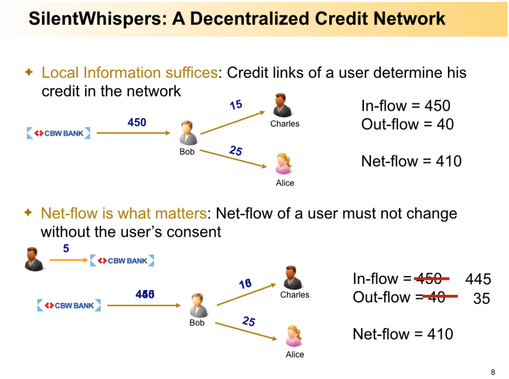
# The Landscape of Emerging Payment Systems

| | Cryptocurrencies | Ripple | SilentWhispers |
|---|---|---|---|
| **Transfer of funds** | Direct transactions between any two wallets | Transactions only via a path with enough credit | |
| **Transaction flexibility** | Fixed currency agreed between sender and receiver | Support for cross-currency transactions | |
| **Transaction verification** | Globally verified | | Locally verified by users in the path |

# Take Home Message

# Take Home Message

- A credit network does not require a global ledger or global consensus



## SilentWhispers: A Decentralized Credit Network

- Local Information suffices: Credit links of a user determine his credit in the network

In-flow = 450
Out-flow = 40

Net-flow = 410

- Net-flow is what matters: Net-flow of a user must not change without the user's consent

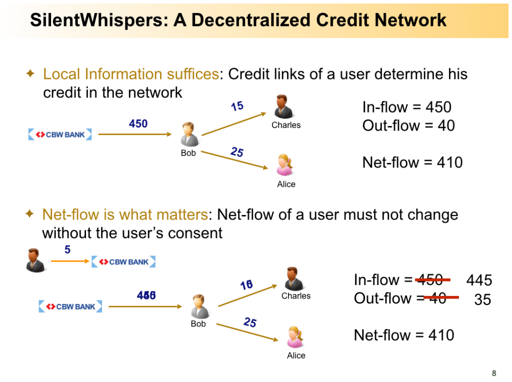
In-flow = ~~450~~ 445
Out-flow = ~~40~~ 35

Net-flow = 410

8

# Take Home Message

- A credit network does not require a global ledger or global consensus



### SilentWhispers: A Decentralized Credit Network

- Local Information suffices: Credit links of a user determine his credit in the network

In-flow = 450
Out-flow = 40

Net-flow = 410

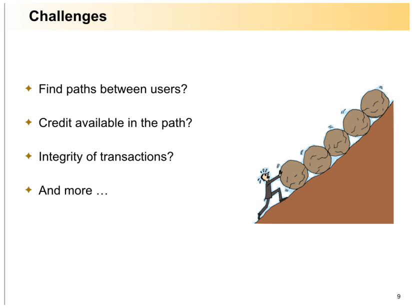
- Net-flow is what matters: Net-flow of a user must not change without the user’s consent

In-flow = ~~450~~ 445
Out-flow = ~~40~~ 35

Net-flow = 410

8

- SilentWhispers: A decentralized credit network enforcing security and privacy and overcoming several challenges



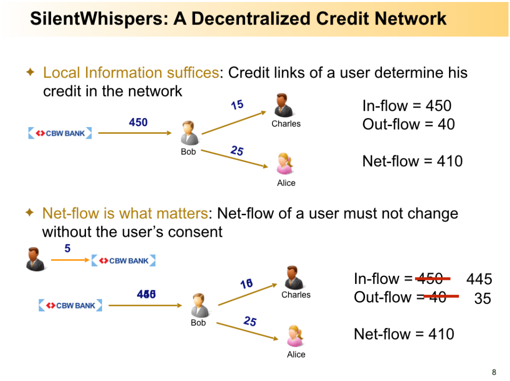
### Challenges

- Find paths between users?
- Credit available in the path?
- Integrity of transactions?
- And more …

9

# Take Home Message

- A credit network does not require a global ledger or global consensus



## SilentWhispers: A Decentralized Credit Network

- Local Information suffices: Credit links of a user determine his credit in the network

In-flow = 450
Out-flow = 40

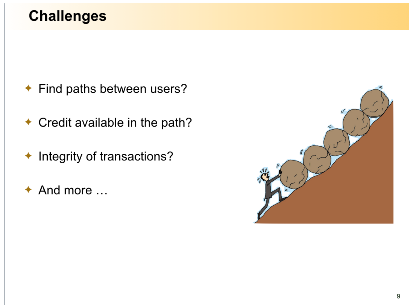
Net-flow = 410

- Net-flow is what matters: Net-flow of a user must not change without the user's consent

In-flow = ~~450~~ 445
Out-flow = ~~40~~ 35

Net-flow = 410

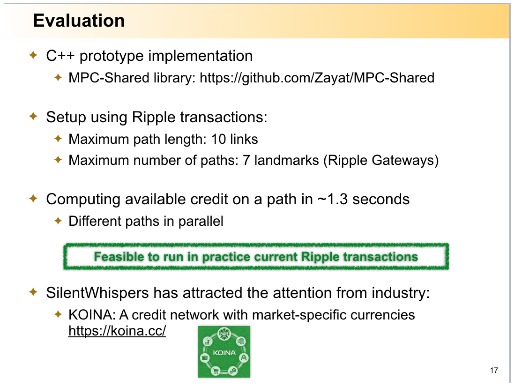
- SilentWhispers: A decentralized credit network enforcing security and privacy and overcoming several challenges



## Challenges

- Find paths between users?
- Credit available in the path?
- Integrity of transactions?
- And more …

- SilentWhispers is feasible in practice and it has attracted attention from industry



## Evaluation

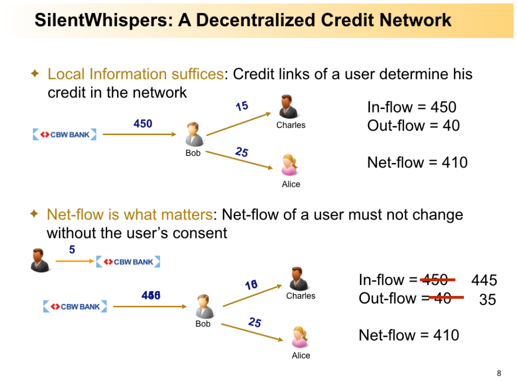
- C++ prototype implementation
  - MPC-Shared library: https://github.com/Zayat/MPC-Shared
- Setup using Ripple transactions:
  - Maximum path length: 10 links
  - Maximum number of paths: 7 landmarks (Ripple Gateways)
- Computing available credit on a path in ~1.3 seconds
  - Different paths in parallel

Feasible to run in practice current Ripple transactions

- SilentWhispers has attracted the attention from industry:
  - KOINA: A credit network with market-specific currencies https://koina.cc/

# Take Home Message

- A credit network does not require a global ledger or global consensus



### SilentWhispers: A Decentralized Credit Network

- Local Information suffices: Credit links of a user determine his credit in the network

In-flow = 450
Out-flow = 40

Net-flow = 410

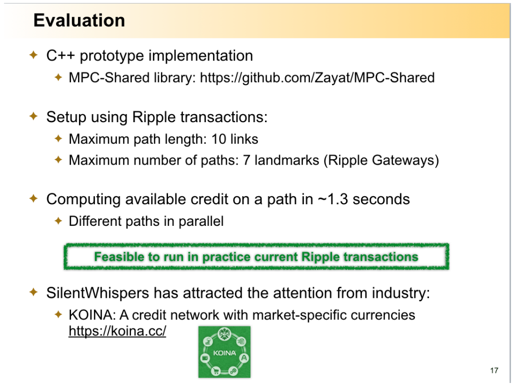
- Net-flow is what matters: Net-flow of a user must not change without the user's consent

In-flow = ~~450~~ 445
Out-flow = ~~40~~ 35

Net-flow = 410

8

- SilentWhispers is feasible in practice and it has attracted attention from industry



### Evaluation

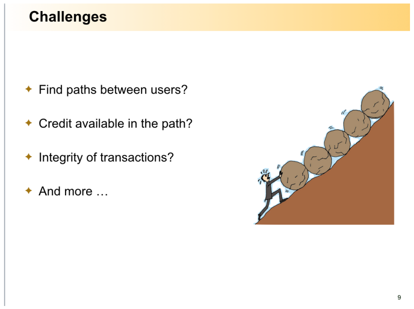
- C++ prototype implementation
  - MPC-Shared library: https://github.com/Zayat/MPC-Shared
- Setup using Ripple transactions:
  - Maximum path length: 10 links
  - Maximum number of paths: 7 landmarks (Ripple Gateways)
- Computing available credit on a path in ~1.3 seconds
  - Different paths in parallel

Feasible to run in practice current Ripple transactions

- SilentWhispers has attracted the attention from industry:
  - KOINA: A credit network with market-specific currencies https://koina.cc/

17

- SilentWhispers: A decentralized credit network enforcing security and privacy and overcoming several challenges

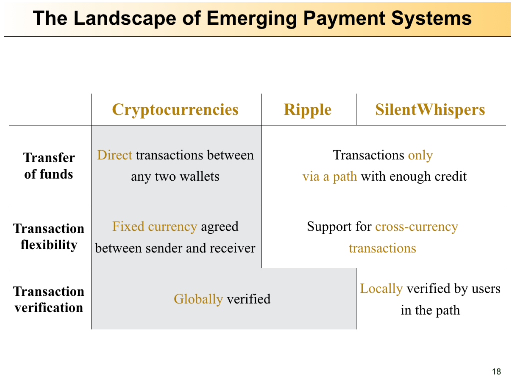


### Challenges

- Find paths between users?
- Credit available in the path?
- Integrity of transactions?
- And more …

9

- SilentWhispers is an interesting alternative in the landscape of emerging payment systems



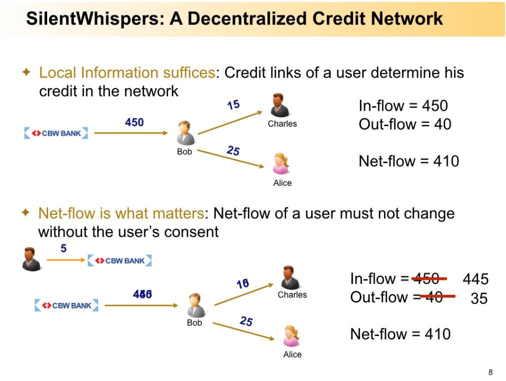
### The Landscape of Emerging Payment Systems

| | Cryptocurrencies | Ripple | SilentWhispers |
|---|---|---|---|
| Transfer of funds | Direct transactions between any two wallets | Transactions only via a path with enough credit | |
| Transaction flexibility | Fixed currency agreed between sender and receiver | Support for cross-currency transactions | |
| Transaction verification | Globally verified | | Locally verified by users in the path |

18

# Take Home Message

- A credit network does not require a global ledger or global consensus



## SilentWhispers: A Decentralized Credit Network

- Local Information suffices: Credit links of a user determine his credit in the network

In-flow = 450
Out-flow = 40

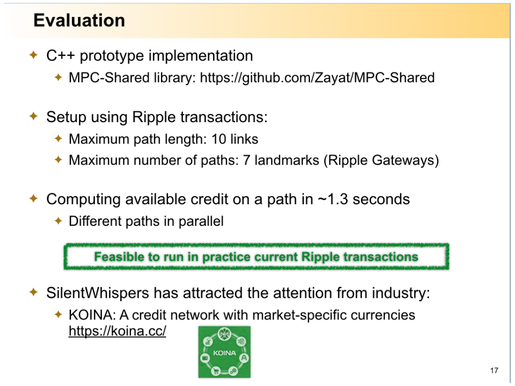
Net-flow = 410

- Net-flow is what matters: Net-flow of a user must not change without the user's consent

In-flow = ~~450~~ 445
Out-flow = ~~40~~ 35

Net-flow = 410

- SilentWhispers is feasible in practice and it has attracted attention from industry



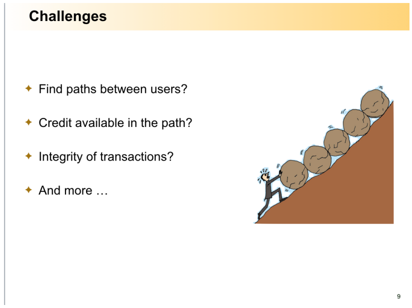
## Evaluation

- C++ prototype implementation
  - MPC-Shared library: https://github.com/Zayat/MPC-Shared
- Setup using Ripple transactions:
  - Maximum path length: 10 links
  - Maximum number of paths: 7 landmarks (Ripple Gateways)
- Computing available credit on a path in ~1.3 seconds
  - Different paths in parallel

**Feasible to run in practice current Ripple transactions**

- SilentWhispers has attracted the attention from industry:
  - KOINA: A credit network with market-specific currencies https://koina.cc/

- SilentWhispers: A decentralized credit network enforcing security and privacy and overcoming several challenges



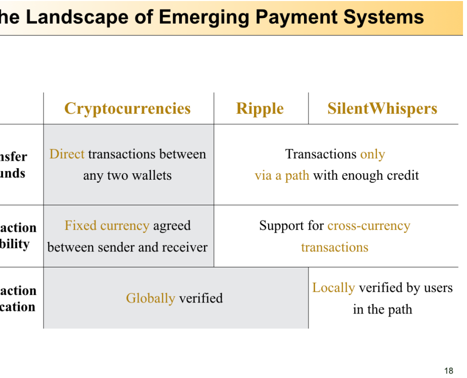
## Challenges

- Find paths between users?
- Credit available in the path?
- Integrity of transactions?
- And more …

***Thanks!***

***@pedrorechez***

- SilentWhispers is an interesting alternative in the landscape of emerging payment systems



## The Landscape of Emerging Payment Systems

| | Cryptocurrencies | Ripple | SilentWhispers |
|---|---|---|---|
| Transfer of funds | Direct transactions between any two wallets | Transactions only via a path with enough credit | |
| Transaction flexibility | Fixed currency agreed between sender and receiver | Support for cross-currency transactions | |
| Transaction verification | Globally verified | | Locally verified by users in the path |